Johann Schmölzer

IT-Sicherheit von SCADA-Systemen

eingereicht als

Diplomarbeit

an der

HOCHSCHULE MITTWEIDA

UNIVERSITY OF APPLIED SCIENCES

Informationstechnik & Elektrotechnik

Graz, 2010

Erstprüfer: Prof. Dr.-Ing. Olaf Hagenbruch

Zweitprüfer: Dipl.-Ing. (FH) Arno Reinhofer

Die vorgelegte Arbeit wurde verteidigt am:

Bibliographische Beschreibung:

Schmölzer, Johann:

IT-Sicherheit von SCADA-Systemen, 75 Seiten, Hochschule Mittweida (FH), Fachbereich Informationstechnik & Elektrotechnik, Diplomarbeit, 2010

Referat:

Diese Diplomarbeit beschäftigt sich mit Aspekten der IT-Sicherheit von SCADA-Systemen. Der Schwerpunkt liegt bei der Bedrohung durch vorsätzliche Handlungen, typischen Schwachstellen und technischen Schutzmaßnahmen. Einführend werden dazu die Grundlagen von IT-Sicherheit und SCADA-Systemen betrachtet. In weiterer Folge wird auf die Besonderheiten von SCADA-Systemen näher eingegangen. Um das Sicherheitsbewusstsein des Lesers zu schärfen, wird das Bedrohungsbild genau analysiert und dargestellt. Typische SCADA-Schwachstellen zeigen die häufigsten Fehler im Bezug auf IT-Sicherheit auf. Mögliche Angriffsszenarien und bekannte sicherheitsrelevante Ereignisse sollen das Bild abrunden. Den Abschluss dieser Arbeit bilden Sicherheitskonzepte und Schutzmaßnahmen, die speziell auf den Einsatz in SCADA-Systemen abgestimmt wurden. Diese Arbeit bildet eine fundierte Basis für die Durchführung eine Risikoanalyse an einem SCADA-System.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

BSI	Bundesamt für Sicherheit in der Informationstechnik – Bundesbehörde der Bundesrepublik Deutschland für Fragen zur IT-Sicherheit in der Informationsgesellschaft
ERP	Enterprise Resource Planning – System zur Planung des Einsatzes von Unternehmensressourcen (Handel, Produktion, Personalwesen …)
HMI	Human Machine Interface – Benutzerschnittstelle, auch MMI (Men Machine Interface)
I/O	Input/Output
ISMS	Information Security Management System - Managementsystem für Informationssicherheit
ISO	International Standardization Organization – Internationales Normungsgremium
IT	Informationstechnik
MIS	Management Information System – Berichts- und Controllingsystem
NIST	National Institute of Standards and Technology – Bundesbehörde der Vereinigten Staaten von Amerika, für Standardisierung zuständig
OE-IT-SIHB	Österreichisches-IT-Sicherheitshandbuch – Herausgegeben vom Bundeskanzleramt
PLC	Programmable Logic Controller – Speicherprogrammierbare Steuerung (SPS)
PLS	Prozessleitsystem
RAS	Remote Access Service
SCADA	Supervisory Control and Data Acquisition

Vorwort

Diese Diplomarbeit entstand im Zusammenhang mit meiner beruflichen Tätigkeit bei der VERBUND – Austrian Hydro Power AG als Systembetreuer von SCADA-Systemen und der Einführung eines neuen Leitsystems in der Zentralwarte Steiermark.

Mein besonderer Dank gilt meinem Erstbetreuer Herrn Prof. Dr.-Ing. Olaf Hagenbruch und meinem Zweitgutachter Dipl.-Ing. (FH) Arno Reinhofer für die kompetente fachkundige Unterstützung.

Des Weiteren möchte ich mich bei Herrn Dipl.-Ing. Josef Schernthanner, der mir für die Erstellung dieser Arbeit die Nutzung der Bildungskarenz ermöglicht hat, bedanken.

Ein herzlicher Dank gilt meiner Familie und meinen Freunden, die sich während meines Studiums sehr verständnisvoll gezeigt und mich in jeder Hinsicht unterstützt haben.

Zu guter Letzt möchte ich mich bei all meinen Arbeitskollegen bedanken, die in der Zeit meiner Abwesenheit Teile meines Aufgabenbereiches übernommen haben.

HERZLICHEN DANK!

1 Einleitung

1.1 Motivation und Ziel

Unsere Gesellschaft ist weitgehend vom Funktionieren der Infrastruktur abhängig. Ohne die gesicherte Versorgung mit Energie und Trinkwasser oder funktionierendes Transportwesen, Informationstechnik und Telekommunikation würde innerhalb kurzer Zeit Chaos ausbrechen. Mit Hilfe von Leitsystemen, sogenannten SCADA-Systemen, werden die hinter der Infrastruktur stehenden technischen Prozesse überwacht und gesteuert. Bedingt durch die Globalisierung und Liberalisierung vieler Märkte haben sich die Anforderungen an diese Systeme in den letzten 10 Jahren stark verändert. Die Leitsysteme werden heute oft mit Office-Systemen vernetzt um Informationen mit übergeordneten Systemen direkt auszutauschen. Dadurch werden die bis dahin abgeschotteten Systeme den Gefahren der modernen IT-Welt ausgesetzt.

Den Anstoß zu dieser Arbeit gab die Einführung eines neuen Leitsystems in der Zentralwarte Steiermark der VERBUND – Austrian Hydro Power AG im Frühjahr 2007.

Diese Diplomarbeit soll als Grundlage für eine zu erstellende IT-Risikoanalyse für das neue SCADA-System der Zentralwarte Steiermark dienen. Dazu sollen die dafür relevanten Aspekte der IT-Sicherheit von SCADA-Systemen betrachtet werden.

1.2 Themenstellende Firma

„*Der **Verbund** ist Österreichs mit Abstand größter Stromerzeuger aus natürlicher und umweltfreundlicher Wasserkraft. Die Erzeugungsgesellschaft des Verbund für Strom aus Wasserkraft ist die **VERBUND-Austrian Hydro Power AG** (AHP). Die **AHP** betreibt 108 Wasserkraftwerke mit einer Maximalleistung von zusammen mehr als 6.000 Megawatt und einer durchschnittlichen jährlichen Erzeugung von rund 22,8 Mrd. kWh. Die AHP ist für Planung, Bau, Betriebsführung und Instandhaltung von Wasserkraftanlagen zuständig.*“ (Verbund, 2009)

Die AHP ist österreichweit organisatorisch in 6 Werksgruppen unterteilt. Die Werksgruppe Steiermark (EPG) ist für den **Betrieb von 40 Wasserkraftwerken** an den Flüssen Mur und Enns sowie deren Zubringern mit einer Jahreserzeugung von ca. 2,5 Mrd. kWh verantwortlich. Die Werksgruppe erzeugt mit knapp 40% aller AHP-Wasserkraftwerke rund 10% des Stroms der gesamten AHP.

Die Fachgruppe Elektro- und Leittechnik (EEL) ist innerhalb der AHP für Planung, Bau, Inbetriebsetzung und Wartung von elektro- und leittechnischen Anlagen zuständig. Der Fachbereich übergeordnete Leittechnik (ÜLT) betreut hierbei das Gebiet der übergeordneten Leitsysteme (SCADA).

1.3 Kapitelübersicht

Kapitel 1 soll in das Thema der Diplomarbeit einführen und einen kurzen Überblick geben, welche Inhalte in den einzelnen Kapiteln der Diplomarbeit abgehandelt werden.

In **Kapitel 2** werden die Grundlagen und der Stand der Technik von IT-Sicherheit und SCADA-Systemen erörtert.

Kapitel 3 zieht ein kurzes Resümee aus den Grundlagen und präzisiert die Aufgabenstellung.

In **Kapitel 4** wird das für SCADA-Systeme bestehende Bedrohungspotenzial analysiert.

Typisch Schwachstellen von SCADA-Systemen werden in **Kapitel 5** untersucht.

In **Kapitel 6** werden Sicherheitskonzepte und -maßnahmen für den Schutz von SCADA-Systemen erörtert.

Kapitel 7 stellt die Ergebnisse dieser Arbeit in kompakter Form dar.

In **Kapitel 8** werden die in dieser Arbeit erreichten Ziele bewertet. Der Ausblick auf die weitere Vorgangsweise im Unternehmen sowie auf mögliche weitere Untersuchungen bildet den Abschluss.

2 Grundlagen

2.1 IT-Sicherheit

Da Unternehmen und Organisationen den größten Teil ihrer Aufgaben mit Hilfe von IT-Systemen bewältigen, sind diese in großem Maß von dessen Funktionieren (Bestand der IT-Grundwerte) abhängig.

Daher müssen laut Federrath (Federrath, et al., 2004 S. 467) IT-Systeme gegen unbeabsichtigte Fehler und Ereignisse und beabsichtigte Angriffe gesichert werden. Dabei gilt es die **Vertraulichkeit**[1], **Integrität**[2] und **Verfügbarkeit**[3] von Informationen zu schützen. Nach dem BSI (BSI-100-1, 2008) werden abhängig vom individuellen Anwendungsfall noch weitere Grundwerte wie Authentizität[4], Verbindlichkeit, Zuverlässigkeit und Nichtabstreitbarkeit hinzugerechnet.

Im englischen Sprachgebrauch wird zwischen **Security** (Schutz vor beabsichtigten Ereignissen) und **Safety** (Schutz vor unbeabsichtigten Ereignissen, technische Sicherheit) unterschieden, im deutschen Sprachraum wird beides als **Sicherheit** bezeichnet.

Diese Arbeit wird sich mit dem im englischen Sprachgebrauch definierten Bereich der Security beschäftigen.

---

[1] Sicherstellung, dass Informationen nur für autorisierte Benutzer zugänglich sind (ISO/IEC 17799)

[2] Sicherung der Richtigkeit und Vollständigkeit der Informationen und ihrer Verarbeitungsmethoden (ISO/IEC 17799)

[3] Sicherstellung, dass autorisierte Benutzer bei Bedarf jederzeit Zugang zu Informationen und verbundenen Informationswerten haben (ISO/IEC 17799)

[4] Echtheit und den Tatsachen entsprechend

In Abbildung 1 sind Begriffe aus der Sicherheit und ihre Beziehung zu anderen Begriffen dargestellt.

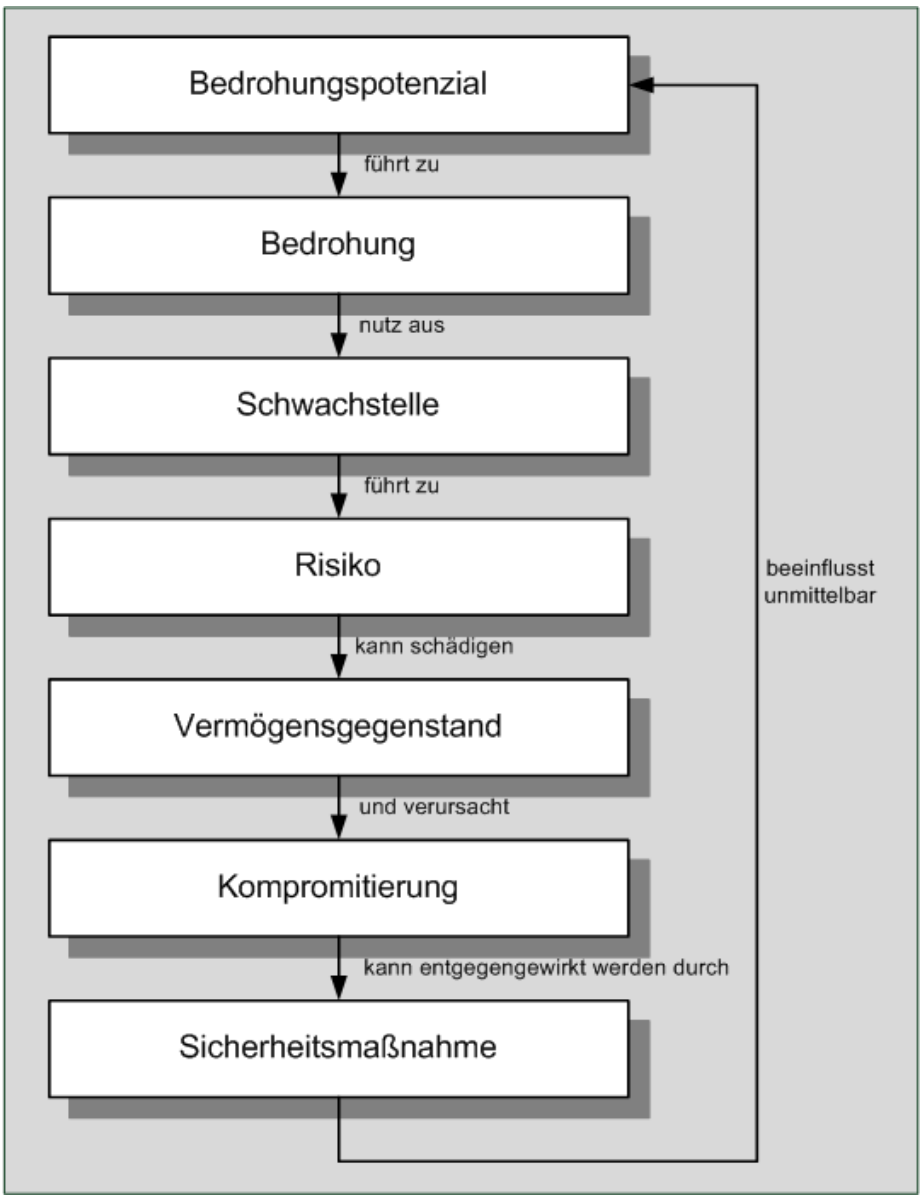

Abbildung 1: Sicherheitsbegriffe und Beziehungen (Meyers, et al., 2007 S. 37)

Das BSI unterscheidet im IT-Grundschutz-Katalog (BSI-GSK, 2009) folgende Gefährdungsarten:

- **Höhere Gewalt** (z.B. Feuer, Wasser, Sturm, Ausfall des Übertragungsnetzes)
- **Organisatorische Mängel** (z.B. fehlende Regelungen, unzureichende Wartung)
- **Menschliche Fehlhandlungen** (z.B. Fehlbedienung, fehlerhafte Administration)
- **Technisches Versagen** (z.B. defekte Datenträger, Stromausfall)
- **Vorsätzliche Handlungen** (z.B. Manipulation von Informationen, Verhinderung von Diensten)

Um die IT-Sicherheit zu gewährleisten, werden dem Bedrohungspotenzial im Rahmen eines **IT-Sicherheitsmanagementsystems (ISMS)** folgende Maßnahmearten entgegen gestellt:

- **Technische Maßnahmen**
- **Organisatorische Maßnahmen**
- **Personelle Maßnahmen**

Das ISMS liegt in der Verantwortlichkeit der Unternehmensleitung und hat als Aufgabe das Definieren, Kontrollieren und Verbessern der IT-Sicherheit.

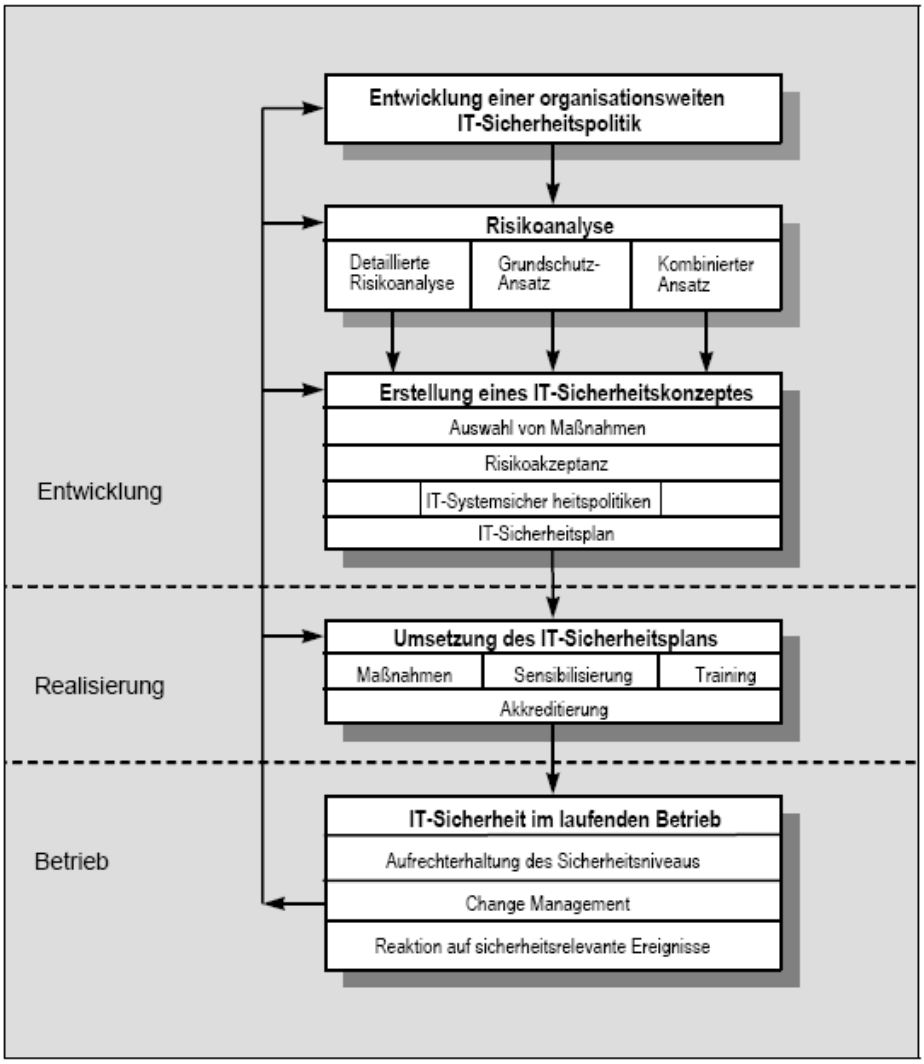

Abbildung 2: Prozesse im IT-Sicherheitsmanagement (OE-IT-SIHB, 2007)

Nach dem Österreichischen IT-Sicherheitshandbuch (OE-IT-SIHB, 2007) ist die Risikoanalyse eine wesentliche Voraussetzung für die Realisierung eines IT-Sicherheitsmanagementsystems. Darin wird versucht, Risiken zu erfassen und zu bewerten, um das Gesamtrisiko für ein IT-System zu erhalten.

Man kann folgende 3 Strategien für die Durchführung einer Risikoanalyse unterscheiden:

- **Detaillierte Risikoanalyse**

  Die ersten Schritte sind dabei die Systembeschreibung und Abgrenzung sowie eine detaillierte Erfassung aller bedrohten Werte. Die weiteren Schritte bestehen aus Wertermittlung, Bedrohungsanalyse, Schwachstellenanalyse, Erhebung bestehender Maßnahmen und abschließender Risikobewertung. Die detaillierte Risikoanalyse benötigt ein hohes Maß an Zeit und Aufwand, wobei eine objektive Wertermittlung und Bedrohungsanalyse oft nur schwer durchführbar ist. Als Vorteil kann der effektive Schutz des Systems angegeben werden.

- **Grundschutzansatz**

  Da eine objektive Feststellung der Bedrohungslage für ein IT-System nur schwer möglich ist, geht der Grundschutzansatz von einer pauschalierten Gefährdungslage aus. Durch sogenannte Grundschutzmaßnahmen nach den BSI-Grundschutz-Katalogen erreicht das betrachtete System schnell und günstig ein relativ hohes Niveau an Sicherheit. Im Rahmen einer Analyse des Systems wird ein Soll-Ist-Vergleich zwischen in Grundschutz-Katalogen empfohlenen und im System bereits umgesetzten Maßnahmen durchgeführt. Dabei entdeckte Mängel müssen beseitigt werden. Bei erhöhtem Schutzbedarf können die Maßnahmen der Grundschutz-Kataloge durch eigene, strengere Maßnahmen ergänzt werden. Die Vorteile des Grundschutzansatzes liegen bei einem schnell erreichbaren Sicherheitsniveau und gleichzeitig geringen Kosten, als Nachteil muss angegeben werden, dass das Sicherheitsniveau für manche Teile des IT-Systems möglicherweise nicht ausreichend ist.

- **Kombinierter Ansatz**

  Beim kombinierten Ansatz werden alle Systeme mindestens durch Grundschutzmaßnahmen gesichert. Durch eine Schutzbedarfsfeststellung werden die Systeme in die Schutzbedarfskategorien niedrig, mittel und hoch eingeteilt. Nur Systeme der Kategorien hoch werden einer detaillierten Risikoanalyse unterzogen. Der kombinierte Ansatz vereint die Vorteile der detaillierten Risikoanalyse und des Grundschutzes.

In weiterer Folge muss das Gesamtrisiko durch die Einführung von Gegenmaßnahmen innerhalb eines Sicherheitskonzeptes auf ein akzeptables Maß gesenkt werden. Dabei hat die Unternehmensleitung in Abhängigkeit von Kosten und Nutzen folgende Möglichkeiten: (Meyers, et al., 2007 S. 46)

- **Reduzierung des Risikos** (Umsetzen von Gegenmaßnahmen)
- **Akzeptanz des Risikos** (keine Aktion)
- **Risikotransfer** (Versicherung)
- **Zurückweisung des Risikos** (Risiko ignorieren)

Mit relativ geringem Aufwand lässt sich ein normales Sicherheitsniveau im Rahmen des IT-Grundschutzes verwirklichen. Der Aufwand steigt für zunehmendes Sicherheitsniveau exponentiell an.

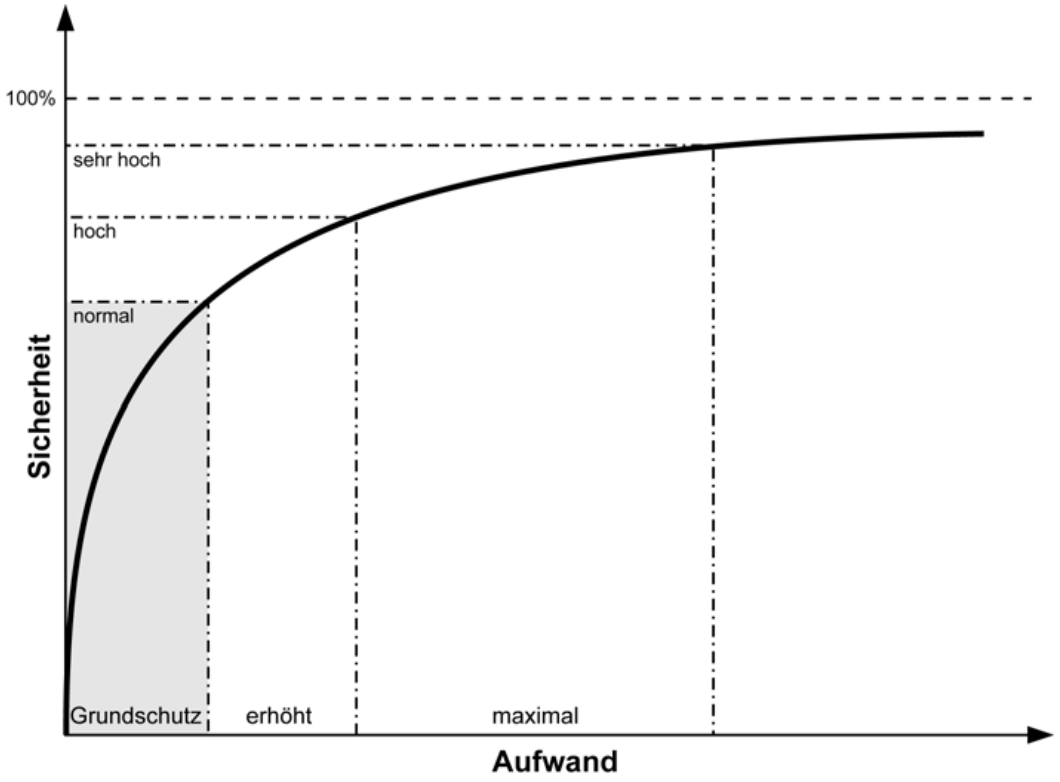

Abbildung 3: IT-Sicherheit Kosten-Nutzen (BSI-100-2, 2008 S. 32)

2.1.1 Stand der Technik

IT-Systeme sind einer sehr großen Anzahl von Gefahren - im Gefährdungskatalog des BSI ersichtlich (BSI-GSK, 2009) - ausgesetzt. Diesen Gefahren steht auch eine nicht minder große Anzahl von Schutzmaßnahmen gegenüber. Um den Umfang dieser Diplomarbeit nicht zu überschreiten, werden nur gebräuchliche technische Schutzmaßnahmen betrachtet.

2.1.1.1 **Zugriffskontrolle**

Bei der Zugriffskontrolle werden laut Meyers (Meyers, et al., 2007 S. 66 ff.) Informationen oder Ressourcen vor unkontrolliertem Zugriff durch Personen oder Geräte geschützt. Es muss sichergestellt werden, dass nicht Autorisierten der Zugriff verwehrt ist und dass Autorisierte keine unerlaubten Änderungen vornehmen können. Die Zugriffskontrolle stützt sich auf folgende 3 Mechanismen:

- **Identifizierung**
  ist ein Vorgang, bei dem einem Authentisierungsdienst eine öffentliche Information zur Identität übergeben wird (z.B. Benutzername, Verfügernummer, Karte …)
- **Authentisierung**
  Bei der Authentisierung wird der private (geheime) Informationsteil zur Feststellung der Identität des Zugreifenden übergeben (z.B. Passwort, Chipkarte, Fingerabdruck …). Damit kann die Authentisierung in die 3 Bereiche **Wissen, Besitz** und **Biometrie** eingeteilt werden.

Wissen	Besitz	Biometrie
Passwort	Smartcard	Fingerscan
PIN	Token Card	Handflächenscan
Antworten auf Fragen	Schlüssel	Irisscan
		Netzhautscan
		Gesichtsgeometrie
		Stimmanalyse
		Handtopologie

Tabelle 1: Authentisierungsmechanismen

Um die Sicherheit der Authentisierung weiter zu erhöhen, werden zwei unterschiedliche Mechanismen miteinander kombiniert (Zwei-Faktor-Authentisierung). Beispiele hierfür sind das Token- und das Smart Card-Verfahren, die Wissen und Besitz-Methoden kombinieren. Biometrische Methoden gelten als sehr sicher, werden von den Benutzern aber häufig wegen Eingriffs in die Privatsphäre abgelehnt.

- **Autorisierung**

  „*Unter Autorisierung versteht man den Prozess der Zuweisung bestimmter Rechte an authentisierte Subjekte, in Abhängigkeit von vorbestimmten Zugriffsrechten und Bewilligungen, die in zugehörigen Zugriffskriterien beschrieben sind. Diese Kriterien werden durch den Administrator oder Sicherheitsbeauftragten entwickelt, um die allgemeine Sicherheitspolitik der Organisation zu unterstützen und in die Tat umzusetzen*." (Meyers, et al., 2007 S. 78)

2.1.1.2 Virenscanner

Virenscanner sind Anwendungen, die Rechner nach Dateien mit bekannten Signaturen von Schadprogrammen (Malware[5]) durchsuchen (scannen). Die Ausführung dieser Dateien wird verhindert oder sie werden vom Rechner entfernt. Dabei können nur bekannte Viren zuverlässig erfasst werden, da die Scanner auf aktuelle Signaturdatenbanken angewiesen sind.

Unter die Kategorie Schadprogramme fallen laut Kaspersky (Kaspersky, 2008 S. 50 ff.):

- **Computerviren**

  Viren sind Schadprogramme, die sich in Dokumenten oder Programmen eingebettet verbreiten, um Daten auf infizierten Rechnern zu verändern oder zu löschen.
- **Computerwürmer**

  Würmer sind Computerviren, die sich über IT-Netzwerke selbstständig verbreiten.
- **Trojaner**

  Trojaner sind Programme, die als Nutzprogramm (z.B. Freeware Tool) getarnt, einem Angreifer unbemerkt Zugang zum befallenen Rechner verschaffen, um Daten auszuspähen, zu ändern oder zu löschen. Auch eine kriminelle Verwendung der Rechnerressourcen für Angriffe auf andere Rechner-Netze (DDoS-Attacke[6]) ist möglich.

Das Online-Scannen eines Rechners benötigt einiges an Rechenkapazität. Dies kann z.B. das Echtzeitverhalten von SCADA-Systemen nachteilig beeinflussen. Durch das sogenannte Blacklist-Verfahren werden definierte Anwendungen von der Ausführung ausgeschlossen. Beim neueren Ansatz des Whitelist-Verfahrens verhält es sich umgekehrt, es dürfen nur definierte Anwendungen ausgeführt werden. Als Vorteil entfällt hierbei das ständige Scannen und die damit verbundene Rechnerbelastung, als Nachteil muss man das Erstellen und Aktualisieren der Whitelist ansehen. (Heise, 2009)

---

[5] Malware ist ein Kunstwort aus malicious (bösartig) und Software

[6] DDoS (Distributed Denial of Service): Gleichzeitige Attacke von mehreren Rechnern auf einen Dienst um diesen zu beeinträchtigen oder zum Absturz zu bringen (z.B. Flut von manipulierten SYN-Anfragen an einen Server)

2.1.1.3 **Firewall**

„*Firewalls bestehen aus einem oder mehreren Rechnern, die TCP/IP-Pakete zwischen einem unsicheren (äußeren) Netz und einem sicheren (inneren) Netz nur dann durchlassen, wenn diese bestimmten Regeln entsprechen (Portnummer, Ziel- oder Quellrechner). Oft erfolgt die Realisierung in Form von zwei Rechnern mit dazwischen liegender „demilitarisierter Zone“ (DMZ). Die Firewall muss für die zulässigen Pakete transparent sein bzw. die Funktion eines Proxy-Servers wahrnehmen. Generell wird empfohlen, dass Computer mit Zugang zum Internet hinter einer Firewall stehen*.“ (Henning, 2004 S. 379 f.)

Dem kann hinzugefügt werden, dass Firewalls auch als reine Softwarelösung mit eingeschränktem Funktionsumfang für Clients existieren (Personal Firewall) und dass die Regeln an der Firewall benutzerabhängig gesteuert werden können. Firewalls arbeiten abhängig von ihrer Ausführung nach unterschiedlichen Methoden:

Die Grundfunktionalität einer jeden Firewall ist die **Paketfilterung,** bei der nur Pakete mit bestimmter Port, Quell- und Zieladresse weitergeleitet werden.

Bei der höherwertigen **Stateful Packet Inspection** überwacht die Firewall zusätzlich die Kommunikation zwischen Client und Server in mehreren OSI-Schichten[7], um nur den vom Client angeforderten Datenverkehr zuzulassen.

Eine **Application Layer Firewall** (ALF) untersucht den Inhalt der Datenpakete der OSI-Schicht 7 (Application Layer) um daraus z.B. Virensignaturen zu erkennen und zu blockieren.

Firewalls sind daher in der Lage, den Informationsaustausch zwischen unterschiedlich vertrauenswürdigen Netzen zu regeln und zu überwachen. Sie schützen ganze Netzwerke oder einzelne Rechner vor unberechtigtem Zugriff und daraus resultierender Manipulation durch Dritte. Sie werden heute in einer Vielzahl von IT-Systemen eingesetzt, schützen aber nur erfolgreich, wenn sie richtig parametriert sind. Nur eine einzige fehlerhafte Regel kann jeglichen Schutz der Firewall zunichtemachen. Daher ist es wichtig, dass lediglich gut ausgebildetes Personal mit der Konfiguration von Firewalls betraut ist.

Firewalls schützen ausschließlich über den Netzwerkverkehr, gegen Bedrohungen die durch mobile Datenträger verursacht werden, z.B. CDs, Disketten, USB-Sticks, mobile Festplatten, Notebooks sowie Mobilfunk-Modems sind sie nur eingeschränkt wirkungsvoll (tlw. Verhinderung der Ausbreitung von Würmern).

[7] Das OSI-Modell (Open System Interconnection) ist ein nach ISO 7498 genormtes Architekturmodel, das die Datenkommunikation zwischen offenen Systemen nach 7 logischen, standardisierten Schichten definiert.

2.1.1.4 Demilitarisierte Zone (DMZ)

Eine DMZ (Demilitarized Zone) ist ein Netzwerksegment, das den sicheren Datenaustausch zwischen einem vertrauenswürdigen und einem weniger vertrauenswürdigen LAN ermöglicht.

Die Funktionsweise einer DMZ wird anhand eines Beispiels nach Abbildung 4 erläutert:

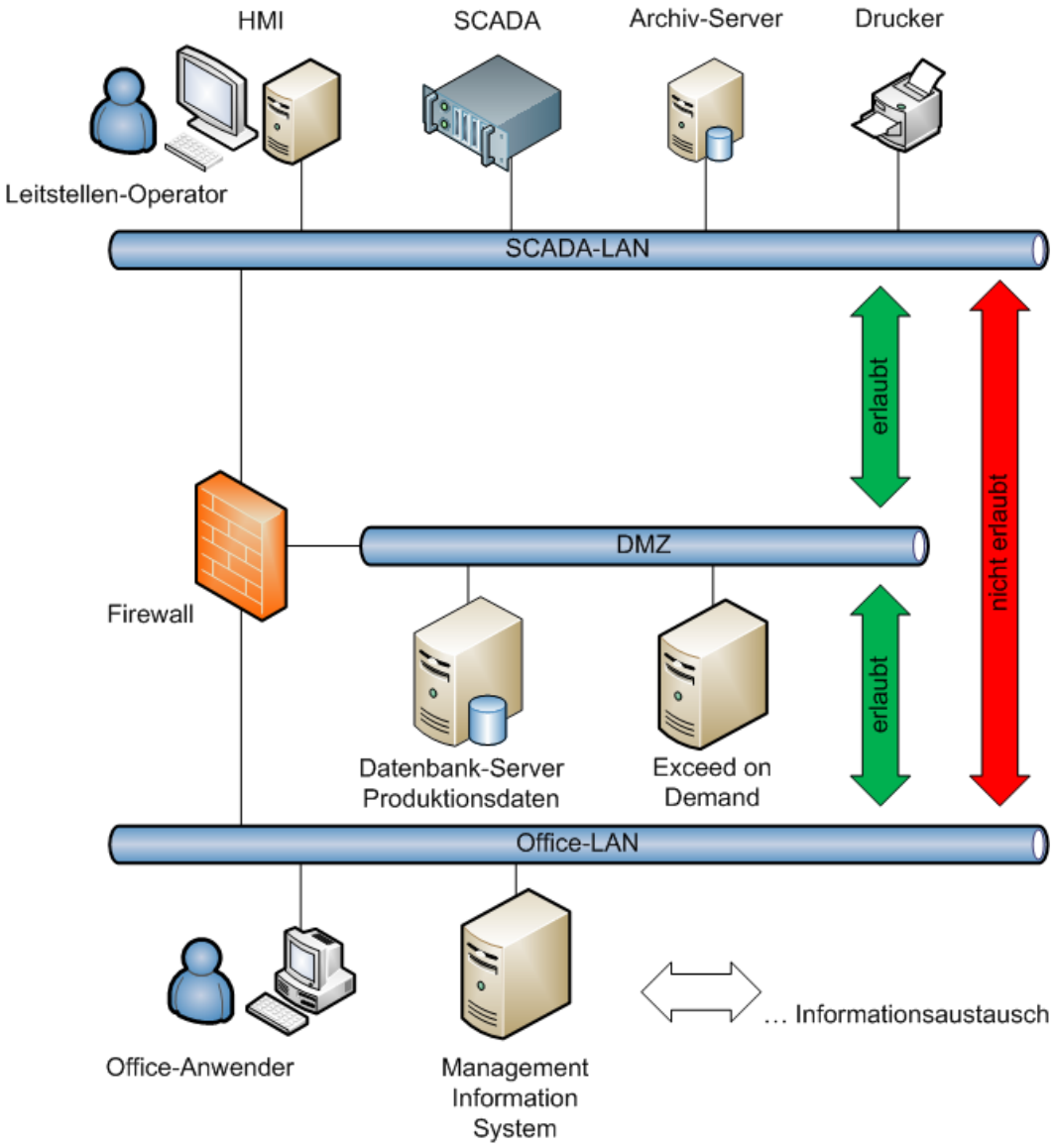

Abbildung 4: Netzwerktopologie einer DMZ

Durch die Schaffung einer DMZ mittels Firewall wird verhindert, dass vom Office-LAN direkt auf das Prozess-LAN zugegriffen werden kann. Umgekehrt ist auch der direkte Zugriff vom Prozess-LAN auf das Office-LAN blockiert. Der Informationsaustausch zischen den beiden Netzen mit unterschiedlicher Vertrauenswürdigkeit kann nur indirekt über das DMZ-LAN erfolgen. So werden z.B. Produktionsdaten des SCADA-Systems am Datenbank-Server in der DMZ abgelegt, von dort kann sie ein Office-Anwender oder ein MIS abrufen.

Die Systeme innerhalb der DMZ sollten als sogenannte Bastion Hosts konfiguriert werden. Das heißt, dass auf ihnen keine unnötigen Dienste oder Subsysteme aktiv sind und keine Fremdanwendungen oder Tools laufen, welche die Sicherheit des Systems beeinträchtigen könnten. Es sollten die aktuellsten Patches installiert und nur die nötigsten Benutzerkonten eingerichtet sein. (Meyers, et al., 2007 S. 227)

Durch einen Dienst- oder Protokollwechsel innerhalb der DMZ wird die Sicherheit zusätzlich weiter erhöht.

2.1.1.5 Intrusion Detection (IDS) und Prevention Systeme (IPS)

„*Als Intrusion-Detection wird die aktive Überwachung von Computersystemen und/oder -netzen mit dem Ziel der Erkennung von Angriffen und Missbrauch bezeichnet. Das Ziel von Intrusion-Detection besteht darin, aus allen im Überwachungsbereich stattfindenden Ereignissen diejenigen herauszufiltern, die auf Angriffe, Missbrauchsversuche oder Sicherheitsverletzungen hindeuten, um diese anschließend vertieft zu untersuchen. Ereignisse sollen dabei zeitnah erkannt und gemeldet werden. […] Als Intrusion-Detection-System wird eine Zusammenstellung von Werkzeugen bezeichnet, die den gesamten Intrusion-Detection-Prozess von der Ereigniserkennung über die Auswertung bis hin zur Eskalation und Dokumentation von Ereignissen unterstützen. Der Großteil marktverfügbare [sic] Intrusion-Detection-Produkte weist diese integrierte Funktionalität auf. IDS können jedoch auch aus Einzelkomponenten zusammengesetzt werden. Auswahl und Zusammenstellung des IDS richten sich dabei nach den individuellen technischen und organisatorischen Gegebenheiten und Anforderungen*.“ (BSI, 2008)

Das Erkennen eines Angriffs hat bei IDS die Dokumentation und Alarmierung des Vorfalles zur Folge. IPS können automatische Gegenmaßnahmen starten wie z.B. aktiv in die Regeln von Firewalls eingreifen und so einen Angriff abwehren.

2.1.1.6 Virtuelles LAN (VLAN)

Mit der VLAN-Technologie ist es möglich, ein physikalisches Netzwerk in mehrere logische Netzwerke (Broadcastdomänen) zu unterteilen und so kontrolliert kommunizieren zu lassen. Dies kann auf unterschiedliche Arten geschehen (Microsoft TechNet, 2006):

- **Statisches VLAN**
  Die Ports eines Switches sind verschiedenen VLANs statisch zugeordnet, beim Anstecken eines Rechners wird dieser automatisch in dem den Port zugewiesenen VLAN Mitglied.

- **Dynamisches VLAN**

  Anhand der MAC-Adresse[8] eines Gerätes oder Benutzerinformationen eines Anwenders wird der betroffene Port des Switches einem VLAN zugewiesen. Die Zuordnung zwischen MAC-Adresse bzw. Benutzerinformation und VLAN muss vom Netzwerkadministrator mithilfe einer Managementanwendung erfolgen. So kann z.B. ein mobiler Arbeitsplatz wie ein Notebook unabhängig von seiner geografischen Position im Netzwerk immer im gleichen VLAN betrieben werden.

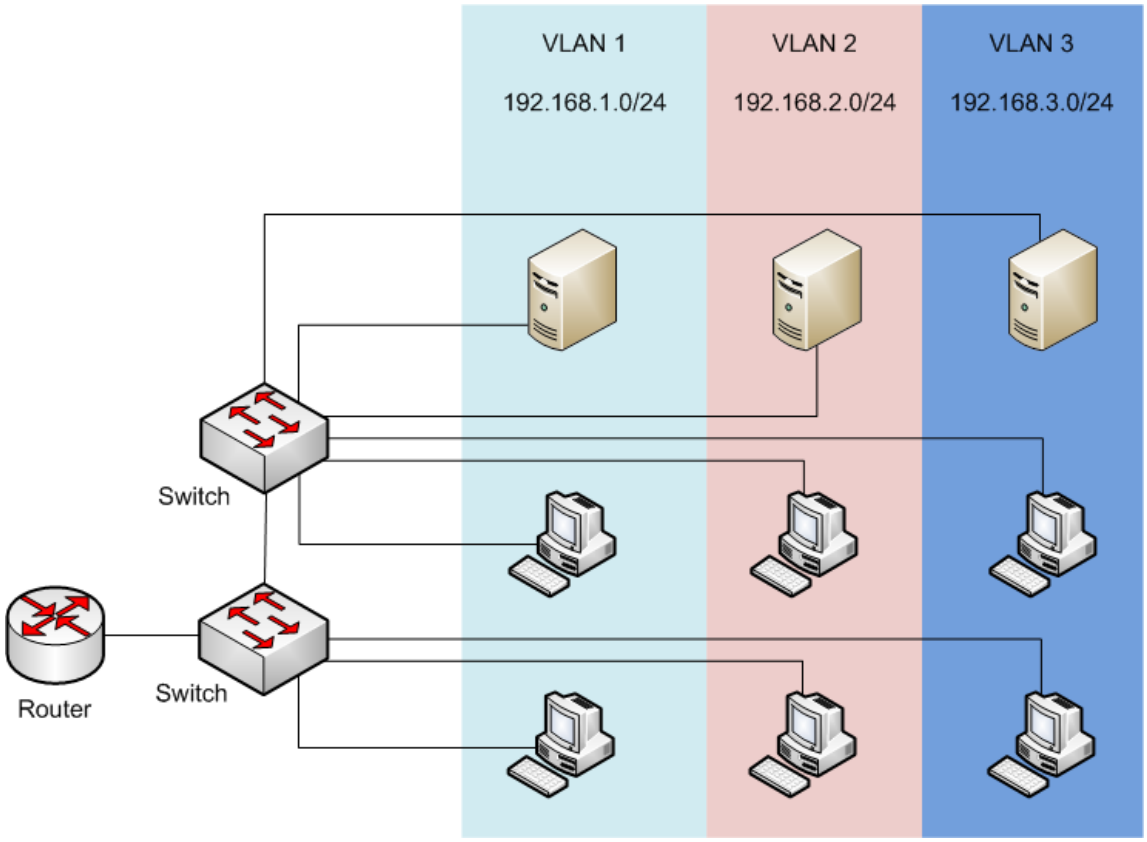

Abbildung 5: Segmentierung durch VLAN-Topologie

In Abbildung 5 ist ein physikalisches Netzwerk, bestehend aus einem Router, zwei Switches und mehreren PCs und Servern, dargestellt. Das Netzwerk ist in 3 VLANs unterteilt, die über den Router oder Layer-3-fähige Switches miteinander kommunizieren können. Die Zuordnung der PCs und Server zu den VLANs ist dabei von der Netzwerkhardware und von der Geografie unabhängig, sie erfolgt rein über die Konfiguration der Geräte. Bei einem herkömmlichen Aufbau müssten die 3 LANs über 3 Hubs oder Switches über einen Router kommunizierend miteinander verbunden werden.

[8] Die MAC-Adresse (Media Access Control) ist die Hardwareadresse eines Gerätes im Netzwerk.

Damit bei der Kommunikation zwischen den Switches die Datenpakete den einzelnen VLANs zugeordnen werden können, müssen die Ethernet-Pakete, abhängig vom eingesetzten Verfahren, um sogenannte VLAN-Tags erweitert oder ganz gekapselt werden (Bündelung). An den Endgeräteports werden die Ethernet-Pakete wieder in ihren ursprünglichen Zustand versetzt.

Für diese Bündelung (Trunking) gibt es mehrere Methoden:

- **IEEE-Standard 802.1Q**

  standardisiertes Verfahren für Ethernet-Switches, bei dem der Frame-Header um einen Tag erweitert wird

- **ISL (Inter-Switch-Link)**
  ist ein schnelles proprietäres Trunking-Protokoll von Cisco für Switches, Router und Netzwerkkarten
- **FDDI 802.10**
  ein für FDDI-Backbones[9] (Fiber Distributed Data Interface) entwickeltes proprietäres Verfahren von Cisco
- **LANE (LAN Emulation)**
  standardisiertes Protokoll für ATM-Verbindungen[10], das dafür sorgt, dass sich ein ATM-Netzwerk wie ein Ethernet-LAN verhält

[9] Fiber Distributed Data Interface ist eine sichere LAN-Technologie auf der Basis von 2 Lichtwellenleiterringen mit dem Token-Ring-Zugriffsverfahren nach ISO 9314. Ein Backbone (Rückgrat) ist der Kern eines LAN, mit dem die wichtigsten Server miteinander verbunden werden.

[10] ATM (Asynchronous Transfer Mode) ist eine asynchrone Übertragungstechnologie von Datenpaketen (Zellen) mit fester Länge nach dem Zeitmultiplexing-Verfahren. Das Haupteinsatzgebiet ist die WAN-Kommunikation.

Die Sicherheitsvorteile von VLANs sind somit die Schaffung von logisch getrennten VLANs innerhalb eines physikalischen LAN (Einschränkung des Zugriffs) und das Verkleinern von Broadcastdomänen (Verringerung der Gefahr durch Broadcast-Stürme[11] z.B. bei einem Smurf-Angriff[12]). Statische VLANs gelten als sicherer, da MAC-Adressen auch gefälscht werden können.

2.1.1.7 **Virtuelles Privates Netz (VPN)**

VPN ist eine Technologie, bei der ein entferntes LAN oder Gerät über einen sicheren Kommunikationstunnel durch ein nicht vertrauenswürdiges Netz angebunden wird.

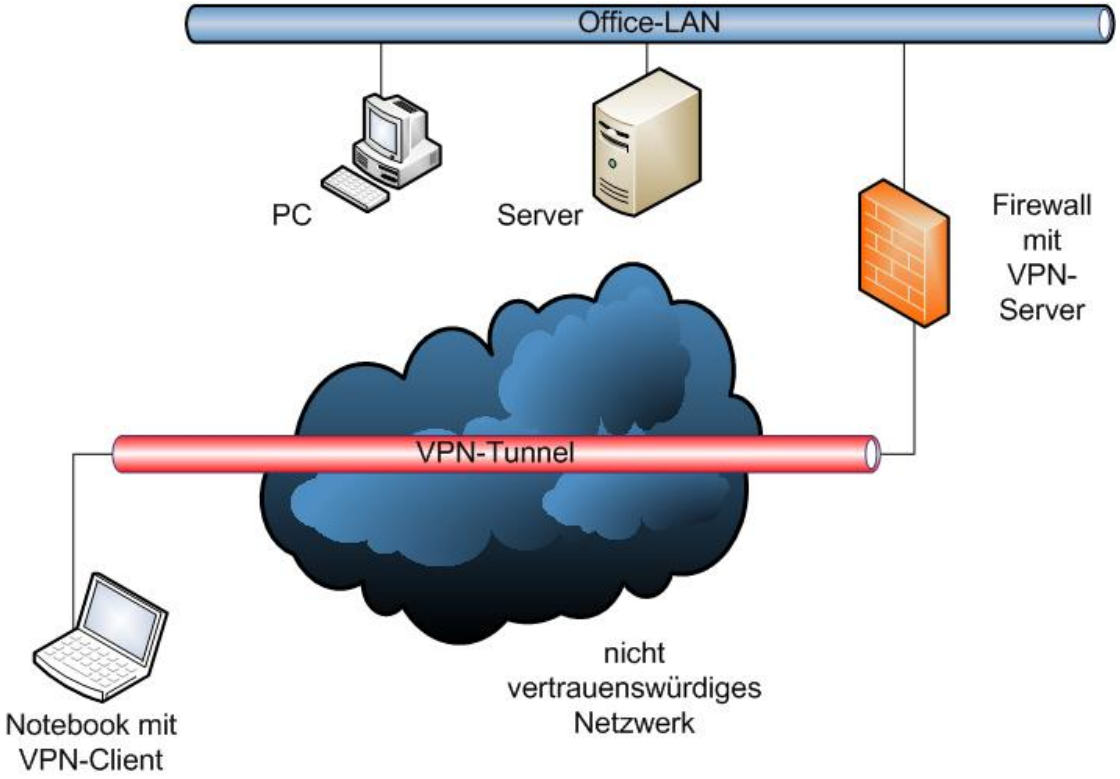

Abbildung 6: VPN-Tunnel

[11] Ein Broadcast-Sturm ist ein erhöhter Datenverkehr innerhalb einer Broadcastdomäne (VLAN bzw. Subnetz) hervorgerufen durch Fehlkonfiguration oder Hacker-Angriff.

[12] „*Ein Smurf-Angriff ist ein DoS-Angriff, der das Internet Control Message Protocol (ICMP) verwendet. Der Angreifer verändert die Quelladresse eines ICMP-ECHO-REQUEST Pakets zur Adresse des Opfers. Wenn ein System ein Echo Request erhält, antwortet es gewöhnlich mit einem Echo Reply. Der Angreifer stellt nun sicher, dass die Zieladresse eine Broadcast-Adresse ist. Wenn nun alle Systeme im Subnetz des Opfers ein Echo Request erhalten, beantworten sie dies mit einem Echo Reply. Das Opfer wird von einer großen Menge ECHO-REPLY-Meldungen überschwemmt und erleidet Performanceeinbußen oder stürzt ab.*“ (Meyers, et al., 2007 S. 454)

Das Notebook in Abbildung 6 kann sich mittels VPN-Client mit dem VPN-Server (Firewall) verbinden und ist nach erfolgreicher Authentisierung ein Mitglied des Office-LAN. Der gesamte Datenverkehr wird hierbei meist verschlüsselt durch den VPN-Tunnel über das nicht vertrauenswürdige Netzwerk wie z.B. das Internet geleitet. Eine Firewall sollte den Datenstrom nach der Entschlüsselung und vor der Übergabe in das interne Netzwerk zusätzlich filtern. (Meyers, et al., 2007 S. 232)

Bei einer VPN-Verbindung werden 3 wichtige IT-Techniken verwendet:

- **Tunneling**

  Ein Gateway kapselt die zu übertragenden Datenpakete in ein Tunnel-Protokoll, das für das Übertragungsmedium geeignet ist und überträgt diese zur Gegenstelle, wo die Pakete wieder ausgepackt werden, um ihren weiteren Weg zu finden.

  Tunnel-Protokolle können aus Sicherheitsgründen einen Verschlüsselungsmechanismus anwenden, bei einem VPN-Tunnel sollte dies unbedingt der Fall sein. (Meyers, et al., 2007 S. 232)

- **Verschlüsselung**

  Bei der Verschlüsselung wird nach Federrath (Federrath, et al., 2004 S. 472 ff.) eine Information mithilfe eines meist bekannten mathematischen Algorithmus und einem privaten Schlüssel in eine unleserliche Form gebracht. Dabei gibt es 2 verschiedene Systeme:

  - **Symmetrisches Verfahren**

    Absender und Empfänger verfügen über den gleichen Schlüssel (z.B. AES)
  - **Asymmetrisches Verfahren** (digitale Signatursysteme)

    Diese Systeme verwenden einen öffentlichen, zertifizierten Schlüssel und einen privaten Schlüssel (z.B. RSA).

  „*Bei hybriden Kryptosystemen wird das asynchrone Verfahren nur zum Austausch eines symmetrischen Sitzungsschlüssels verwendet, während das effiziente symmetrische Verfahren zur Verschlüsselung des Nachrichteninhalts eingesetzt wird*." (Federrath, et al., 2004)

  VPN-Verbindungen werden häufig auf der Basis von IPsec oder SSL übertragen.

- **Authentisierung**

  Mobile Clients, die über eine VPN-Verbindung mit dem Unternehmensnetzwerk kommunizieren, verwenden meist eine Zwei-Faktor-Authentisierung (siehe Absatz 2.1.1.1). Dabei muss der Anwender z.B. eine PIN (Personal Identification Number) oder Passwort und den Besitz eines Gegenstandes wie z.B. eine Token Card oder Smart Card nachweisen.

2.1.2 Normen und Standards

Eine Vielzahl von Normen, Standards und Leitfäden beschäftigen sich mit IT-Sicherheit bzw. IT-Sicherheitsmanagementsystemen. Hier ein kurzer Überblick über die für diese Arbeit maßgeblichen Institutionen und deren Publikationen:

2.1.2.1 **ISO**

Die ISO (International Organisation for Standardization) ist ein Netzwerk aus 162 nationalen Normungsinstituten mit Sitz in Genf. Sie ist der größte Entwickler und Herausgeber von Internationalen Normen. (ISO, 2009)

Die Normenreihe ISO/IEC 27000, gemeinsam mit der IEC[13] herausgegeben, beschäftigt sich mit dem Thema der Informationssicherheit. Die Normenreihe dient als Basis für viele weiterführende Empfehlungen und Leitfäden anderer Organisationen wie z.B. die des BSI.

2.1.2.2 **BSI**

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist eine deutsche Bundesbehörde im Geschäftsbereich des „Bundesministerium des Innern“. Es ist für alle Bereiche der IT-Sicherheit Deutschlands zuständig. Es gliedert sich in die Abteilungen (BSI, 2009c):

- Sicherheit in Anwendungen, kritischen Infrastrukturen (siehe Absatz 2.3) und im Internet
- Kryptographie und Abhörsicherheit
- Zertifizierung, Zulassung und Konformitätsprüfungen, Neue Technologien
- Verwaltung

Das BSI ist eine international äußerst anerkannte, unverzichtbare Quelle von praxisorientierten Leitfäden zum Thema Informationssicherheit.

[13] IEC (International Electrotechnical Commission): Internationale Normungsstelle für Elektrotechnik

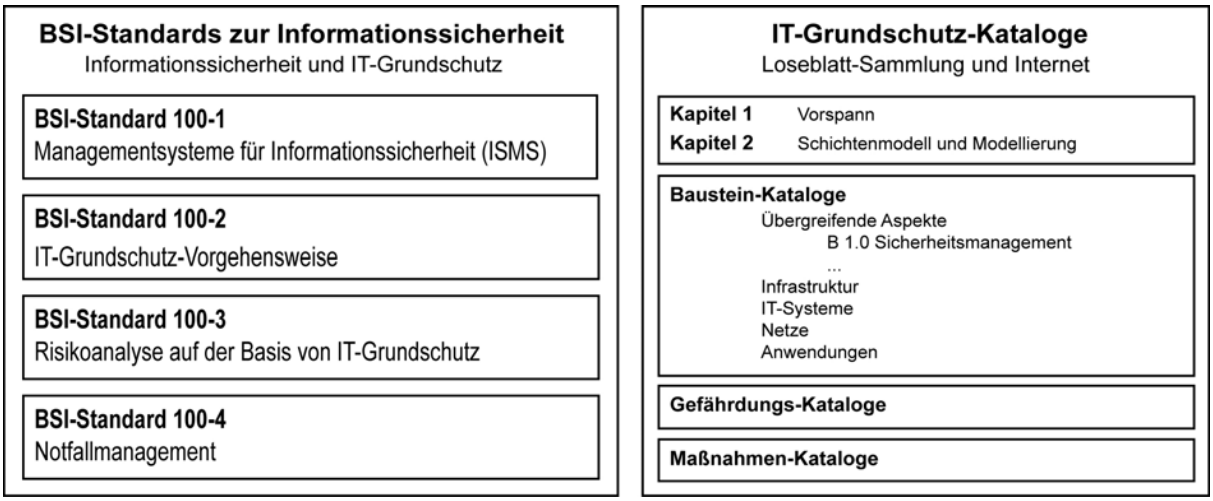

Abbildung 7: BSI-Publikationen zum Sicherheitsmanagement (BSI-100-1, 2008)

Die wichtigsten Publikationen sind in Abbildung 7 dargestellt und werden in weiterer Folge kurz beschrieben:

- **Standard 100-1 - Managementsysteme für Informationssicherheit (ISMS)**
  ist eine leicht verständliche Umsetzung der ISO 27001 Norm, definiert die allgemeinen Anforderungen eines ISMS
- **Standard 100-2 - IT-Grundschutz-Vorgehensweise**
  praxisorientierte Beschreibung für den Aufbau und den Betrieb eines ISMS nach den ISO Normen 27000, 27001 und 27002
- **Standard 100-3 - Risikoanalyse auf der Basis von IT-Grundschutz**
  für die Durchführung einer erweiterten Sicherheitsanalyse bei bestehendem IT-Grundschutz
- **Standard 100-4 - Notfallmanagement**
  Anleitung für Aufbau und Aufrechterhaltung eines Notfallmanagements
- **IT-Grundschutz-Kataloge**
  ist eine praxisorientierte Sammlung von Bausteinen zur ISMS, die konkrete technische Gefährdungen und Gegenmaßnahmen beinhaltet

Das vom BSI vertriebene „GSTOOL“ ist eine Datenbankanwendung, die den Benutzer bei der Durchführung einer Risikoanalyse unterstützt.

2.1.2.3 **NIST**

Das NIST (National Institute of Standards and Technology) ist eine bundesstaatliche Normungsagentur der Vereinigten Staaten von Amerika.

Die Abteilung „Computer Security Division“ hat im September 2008 einen für diese Diplomarbeit relevanten Leitfaden veröffentlicht. Die „**Special Publication 800-82 (Final Public Draft), Guide to Industrial Control Systems (ICS) Security**“ befindet sich zwar noch im erweiterten Entwurfsstatus, bietet aber auch jetzt schon einen guten Überblick über SCADA-Systeme betreffende Aspekte der IT-Sicherheit. Die SP800-82 unterstützt Entwickler und Betreiber von Automatisierungssystemen sowohl bei der Entwicklung wie auch beim Einsatz von Sicherheitskonzepten.

Dieser Leitfaden ist somit einer der wenigen aus dem Bereich der IT-Sicherheit, der sich explizit mit der Sicherheit von SCADA-Systemen beschäftigt.

Weitere ausgewählte Publikationen des NIST im Zusammenhang mit der Sicherheit von SCADA-Systemen sind:

- **Special Publication 800-40**
  Creating a Patch and Vulnerability Management Program
- **Special Publication 800-41**
  Guidelines on Firewalls and Firewall Policy
- **Special Publication 800-77**
  Guide to IPsec VPNs
- **Special Publication 800-94**
  Guide to Intrusion Detection and Prevention Systems (IDPS)
- **Special Publication 800-114**
  User’s Guide to Securing External Devices for Telework and Remote Access
- **Special Publication 800-123**
  Guide to General Server Security

2.2 SCADA-Systeme

SCADA-Systeme (Supervisory Control and Data Acquisition) erlauben es, technische Prozesse zu Überwachen und zu Steuern. Üblicherweise werden mit SCADA-Systemen weit verteilte Prozesse zentral in Leitstellen überwacht, wobei Entscheidungen nicht vom System sondern vom Operator getroffen werden. Diese Eigenschaft unterscheidet SCADA-Systeme von Prozessleitsystemen (PLS), die dezentral z.B. in Kraftwerken eingesetzt werden und autark Entscheidungen treffen.

Die Position des SCADA-Systems innerhalb des Automatisierungsprozesses ist in Abbildung 8 ersichtlich.

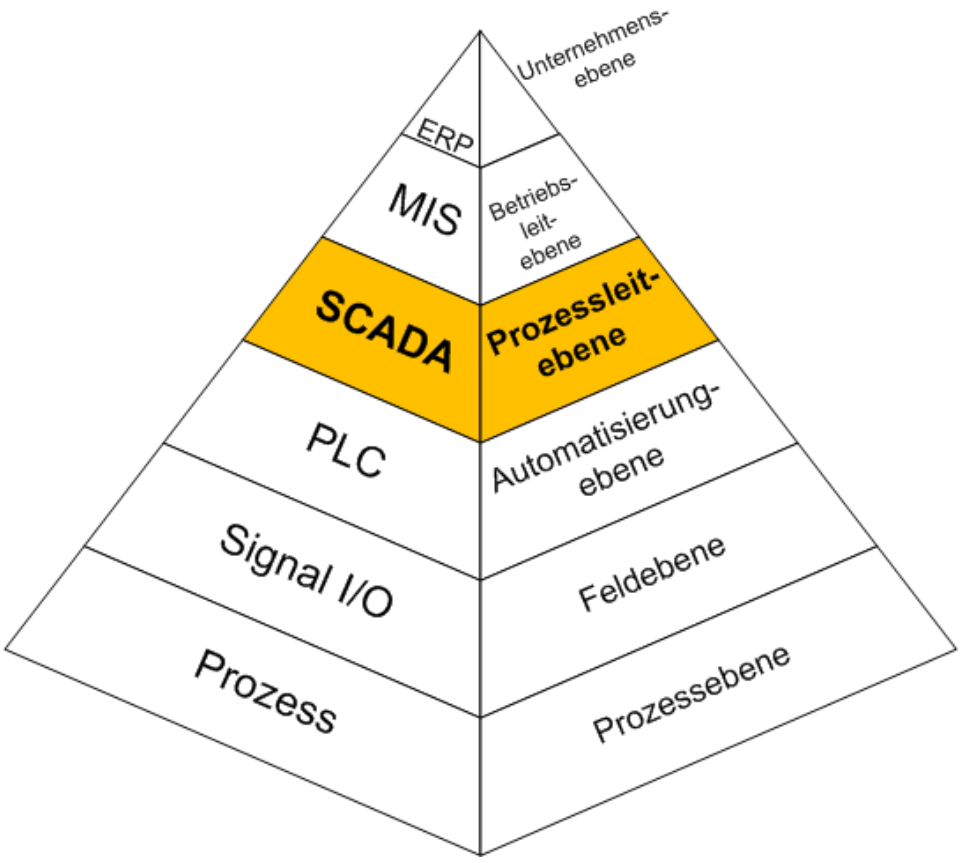

Abbildung 8: Automatisierungspyramide

Die Prozessleitebene kommuniziert mit der untergeordneten Automatisierungsebene über definierte Schnittstellen und erhält so Meldungen, Messwerte und Zählerstände in Melderichtung. Befehle und Sollwerte werden in Befehlsrichtung an prozessnahe Automatisierungskomponenten geschickt. Die übergeordnete Betriebsleitebene wird von der Prozessleitebene mit den wichtigsten Produktionsdaten versorgt, um daraus dem SCADA-System z.B. einen Fahrplan für die weitere Produktion zu übermitteln.

Die Grundfunktionen eines SCADA-Systems sind:

- Prozessvisualisierung
- Meldungs-, Messwert- und Zählwertverarbeitung
- Befehls- und Sollwertgaben
- Alarmierung
- Protokollierung und Archivierung

Häufig sind diese Funktionen in Abhängigkeit der Komplexität des Prozesses auf einen oder mehrere Rechner verteilt, man spricht dann von einem verteilten System (siehe Absatz 2.2.4).

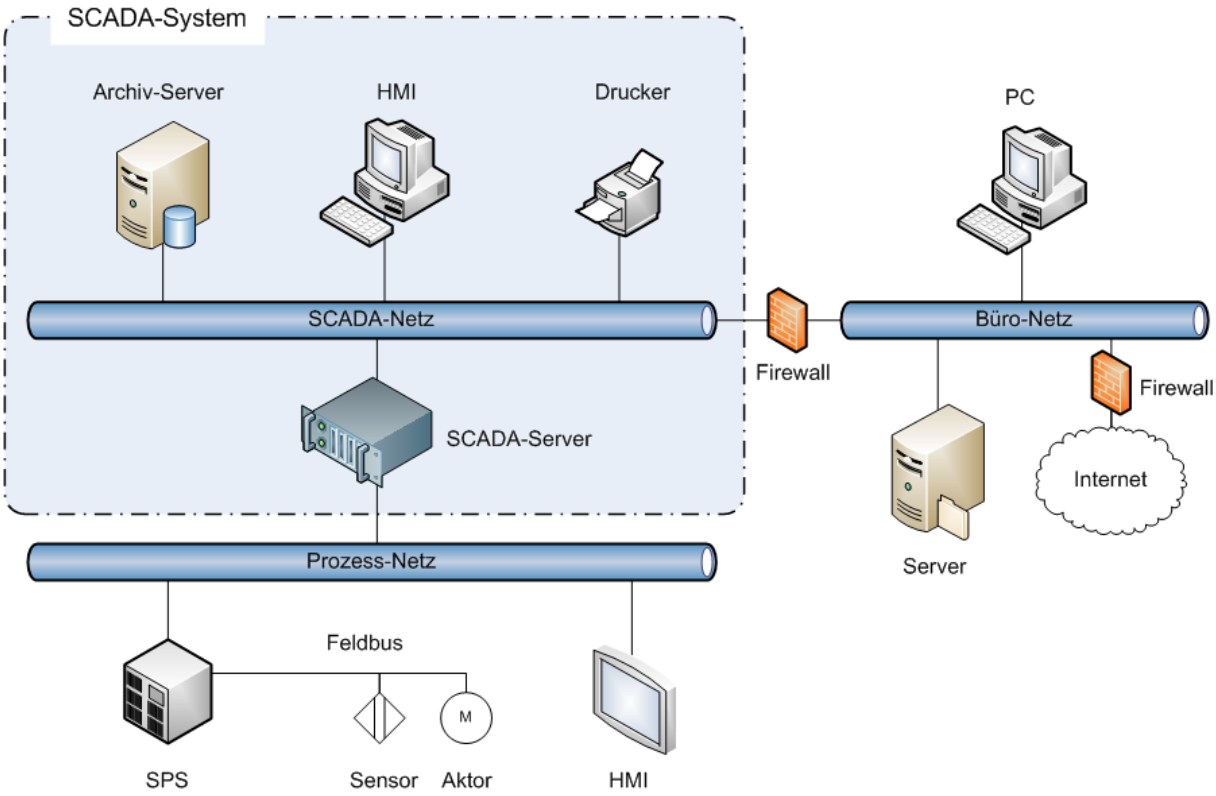

Abbildung 9: Netzwerktopologie eines SCADA-Systems

2.2.1 Anforderungen an SCADA-Systeme

Laut Tauchnitz (Tauchnitz, et al., 2008 S. 191 ff.) sind folgende Eigenschaften von herausragender Wichtigkeit:

- **Verfügbarkeit**

  Durch die Bereitstellung von Redundanzen muss ein möglichst unterbrechungsfreier Betrieb gewährleistet sein. Dies kann durch die doppelte Ausführung von Stromversorgungen, Servern, ganzen Arbeitsplätzen, Kommunikationsmitteln und -wegen usw. erfolgen. Beim Ausfall einer Komponente kann so eine Reservekomponente deren Arbeit übernehmen.

- **Echtzeitfähigkeit**

  Das System muss innerhalb einer definierten Zeitspanne auf Ereignisse reagieren können. Beim Eintreffen einer alarmierenden Meldung (Störung oder Alarm) muss innerhalb einer definierten Zeit ein Eintrag in der Alarmliste erfolgen. Dieser Vorgang darf nicht durch andere Aufgaben, wie z.B. gleichzeitiger Ausdruck eines Protokolls, verzögert werden. Grundsätzlich wird die Echtzeitfähigkeit eines Systems mit der Nähe zum Prozess wichtiger.

- **Offenheit und Interoperabilität**

  Schnittstellen und Systemeigenschaften müssen offengelegt werden oder sich nach einem offengelegten Standard richten. Komponenten verschiedener Hersteller müssen ohne großen Aufwand miteinander betrieben werden können. Offenheit und Interoperabilität sind sehr wichtige Eigenschaften von SCADA-Systemen in der Netz- und Kraftwerksleittechnik, da hier meist große heterogene Systeme unterschiedlicher Hersteller betrieben werden.

- **Durchgängigkeit**

  Trotz der Anschaltung von unterschiedlichen Komponenten und einer Vielzahl von internen Schnittstellen muss für den Anwender ein homogenes System entstehen. Prozessinformationen, die dem System bekannt sind, müssen jeder Komponente ohne großen Aufwand zugänglich sein.

2.2.2 Historische Entwicklung

Die **Entwicklung** von vielen heute noch in Betrieb stehenden SCADA-Systemen geht häufig bis in die 70er und 80er Jahre des 20. Jahrhunderts zurück, dabei lag das Hauptaugenmerk auf der Zuverlässigkeit, Wartbarkeit und Verfügbarkeit der Systeme. Die Systeme arbeiteten auf der Basis von **proprietärer Soft- und Hardware**, die Anschaltung der Prozessebene erfolgte über Datenkonzentratoren und seriellen **Punkt zu Punkt-Verbindungen**. Es waren **autarke Systeme,** die mit speziellem, nur schwer zugänglichem Fachwissen ohne Verbindung zu anderen Netzen oder Systemen betrieben wurden. Als Plattform dienten meist herstellereigene **unixartige Betriebssysteme**, die SCADA-Systeme selbst wurden für den Kunden meist stark angepasst. Der allgemeine Verbreitungsgrad von Rechnern und PCs war noch nicht so stark, die Gesellschaft in einem geringeren Maß von ihnen abhängig. Hacking und Virenentwicklung steckten noch in den Kinderschuhen, das damit verbundene **Bedrohungspotenzial für IT-Systeme war noch gering**. Aus diesen Gründen wurde von den Entwicklern auf eine durchgehende Sicherheitskonzeption verzichtet. Die Sicherheitsmaßnahmen bei den Betreibern beschränkten sich häufig auf den **Schutz vor physikalischen Zugriff**.

Heute setzen SCADA-Systeme **standardisierte Hard- und Softwarekomponenten** wie z.B. den TCP/IP-Netzwerkdienst oder Oracle-Datenbanken ein. Als Plattform dienen hauptsächlich **Microsoft Windows Betriebssysteme**. Die Kommunikation mit der Prozessebene erfolgt mit **IP-Protokollen über Ethernet**. Auf Grund von gestiegenen Anforderungen an den Prozess sind die Systeme mit dem **Office-Netzwerk** der Unternehmen verbunden. Bestehende Systeme wurden aus Kostengründen oft **nur um Konnektivität erweitert**, **ohne** das **Sicherheitskonzept** anzupassen. Die Grenzen zwischen gebräuchlicher Office-IT und den IT-Systemen der Produktionstechnik verschwinden zusehends. Den Technikern in der Automatisierungstechnik fehlt aber oft das Wissen und Sicherheitsbewusstsein das nötig wäre, um auf das dadurch entstandene Bedrohungspotenzial entsprechend zu reagieren. (Wiles, et al., 2007 S. 62 ff.)

2.2.3 Unterschiede zwischen Office- und Produktions-IT

Produktions-IT (und damit auch SCADA-Systeme) unterscheidet sich von Office-IT in einer Vielzahl von Kategorien wie z.B. unterschiedliche Prioritäten, Risiken und Eigenschaften. Ausfälle oder Störungen können Leib und Leben bedrohen, die Umwelt schädigen oder große finanzielle Schäden für Unternehmen oder Organisationen bedeuten. Aus diesem Grund ist die Aufrechterhaltung der Kontrolle über den Prozess von höchster Wichtigkeit. Der ordnungsgemäße Betrieb muss auch beim Auftreten eines Sicherheitsereignisses gewährleistet bleiben.

Kategorie	**Office-IT**	**Produktions-IT**
Performance	Nichtechtzeitverhalten, Antwort muss konsistent sein, Hoher Datendurchsatz, Große Verzögerungen und Schwankungen können akzeptabel sein	Echtzeitverhalten, Antwort ist zeitkritisch, Mäßiger Datendurchsatz, Große Verzögerungen und Schwankungen sind nicht akzeptabel
Verfügbarkeit	Kurze Ausfälle sind meist tolerierbar, Reboot ist meist akzeptabel	Reboot meist nicht akzeptabel, Verfügbarkeitsanforderungen können redundante Systeme erfordern, Abschaltungen müssen langfristig geplant werden
Risikomanagement	Vertraulichkeit und Integrität stehen an erster Stelle, Kurzzeitiger Ausfall tolerierbar, Hauptrisiko ist Verzögerung oder Ausfall von Geschäftsprozessen	Personen- und Anlagenschutz haben Priorität, Kurzzeitiger Ausfall nicht tolerierbar, Hauptrisiko ist der Verlust von Menschenleben, die Verletzung von Gesetzen und Vorschriften, Umweltbeeinflussung, Produktionsausfall
Lebensdauer	3-5 Jahre	15-20 Jahre
Sicherheitsarchitektur	Fokus auf Schutz der IT-Anlagen und Informationen	Hauptziel ist Schutz der Automatisierungsebene und deren Aufgabe

Kategorie	Office-IT	Produktions-IT
Unbeabsichtigte Security-Auswirkungen	Sicherheitslösungen für herkömmliche IT entwickelt und getestet	Sicherheitswerkzeuge müssen auf Betriebssicherheit getestet werden
Zeitkritische Bedienung	kaum zeitkritische Bedienungen, starke Zugriffskontrolle implementiert	schnelle Notfallbedienung ist wichtig, Zugriffskontrolle darf Bedienung nicht behindern
Betriebssystem	Systeme arbeiten mit Standardbetriebssystemen, Unkomplizierte automatisierte Upgrades	Unterschiedliche auch proprietäre Betriebssysteme tw. ohne Sicherheitskonzeption, Upgrades meist nur durch den Lieferanten, Gewährleistung
Performancegrenzen	Systeme haben genug Leistungsreserven um Sicherheitsanwendungen zu unterstützen	Systeme primär für Prozess ausgelegt, für Sicherheitsanwendungen tw. zu wenig Leistungsreserven
Kommunikation	Standardkommunikationsprotokolle, Primär verkabelte Netze und tw. Wireless-LAN, Herkömmliche IT-Netzwerke und Methoden	Standard- und viele proprietäre Kommunikationsprotokolle, Unterschiedliche Kommunikationsmedien, Komplexe Netzwerke
Change-Management	Softwareänderungen und Patches im Rahmen der Sicherheitsrichtlinie, oft automatisiert	Softwareänderungen und Patches müssen sorgfältig getestet und implementiert werden, Wahrung der Integrität des Systems sehr wichtig
Zugänglichkeit	Komponenten normalerweise leicht zugänglich	Komponenten in industrieller Umgebung tw. schwer zugänglich oder weit entfernt

Tabelle 2: Vergleich Office-IT und Produktions-IT (NIST SP800-82, 2008)

2.2.4 Verteilte Systeme

„*Ein verteiltes System besteht aus unabhängigen, über ein Rechnernetz kommunizierenden Rechnern, wobei keine zentrale Systemsteuerung existiert und der Verteilungsaspekt für den Benutzer des Systems möglichst transparent ist*." (Oechsle, 2004 S. 389)

Die Vorteile von verteilten Systemen zeigen sich durch:

- Höhere Rechenleistung durch Verteilung der Aufgaben auf mehrere Rechner
- Höhere Verfügbarkeit durch Redundanzen
- Nutzung gemeinsamer Daten
- Bessere Skalierbarkeit
- Gemeinsame Nutzung von Geräten

Für den Benutzer soll sich ein verteiltes System möglichst als ein einheitliches zentrales System darstellen, man spricht dann von Verteilungstransparenz.

Bei SCADA-Systemen werden typischerweise Anwendungen (Blockfunktionen) auf Rechner verteilt (Anwendungstransparenz).

Typische Blockfunktionen sind:

- Echtzeit-Prozessdatenverarbeitung (z.B. Grenzwertalarmierung)
- Archivierung (Langzeitarchivierung von Meldungs- und Messwertdaten)
- Engineering (Datenmodell der Prozessdaten und Visualisierung)
- Grafische Benutzerschnittstelle (HMI)

2.2.5 Stand der Technik

SCADA-Systeme sind heute in allen Bereichen der Fertigung, Industrie und Infrastruktur zu finden. Mit ihnen werden z.B. kleine Fertigungsmaschinen oder auch große Stromnetze eines ganzen Staates überwacht und gesteuert. Dementsprechend gibt es eine große Anzahl von Anbietern, die SCADA-Systeme für die unterschiedlichsten Einsatzbereiche entwickelt haben. Das Spektrum reicht von einem HMI-System einer Fertigungsmaschine, das auf einem industrietauglichen Windows CE-Touchpanel läuft, bis zu einem verteilten Netzleitsystem, das mit dutzenden Servern und HMI-Clients über ein ganzes Land verstreut ein Stromnetz mit mehreren hunderttausend Datenpunkten überwacht.

SCADA-Systeme sind meist nach dem **Client-Server-Prinzip** aufgebaut. Ein Client (z.B. HMI) fordert (Request) von einem Server (z.B. SCADA-Server) eine Dienstleistung (z.B. Daten aus dem Messwertarchiv) an. Der Server bearbeitet den Auftrag und schickt die Daten an den Client zurück (Response). Dieses in der IT bewährte Prinzip ermöglicht einen modularen Aufbau von Anwendungen und ist somit wirtschaftlich, flexibel und erlaubt die Einbindung von Standardanwendungen. (Oechsle, 2004 S. 400)

Die **Kommunikation** mit der Automatisierungsebene kann dabei z.B. mit Feldbusprotokollen wie PROFIBUS-DP oder mit TCP/IP-Protokollen wie IEC 60870-5-104 über LAN/WAN erfolgen, wobei bestehende Feldbus-Technologien zunehmend durch Ethernet-Protokolle (TCP/IP, EtherNet/IP, Powerlink, Profinet IO usw.) abgelöst werden. (HMS, 2009) Prinzipiell nimmt der Aspekt der Kommunikation im Energiesektor eine besonders wichtige Rolle ein. Das Datenübertragungsnetz und das Leitsystem müssen in der Lage sein, räumlich weit verteilte Anlagen wie Kraftwerke, Schaltanlagen, Umspannwerke, Trafo- und Messstationen unterschiedlichster Technologien effizient und kostengünstig zu vernetzen. In der Netzleittechnik geht der Trend von der signalorientierten zur objektorientierten Datenübertragung nach IEC 61850. Dabei wird in einem Telegramm nicht nur mehr eine Information, sondern der gesamte Prozesszustand eines Objektes wie z.B. eines Leistungsschalters übertragen.

Moderne homogene Automatisierungssysteme unterstützen **durchgängiges Engineering** von der Feld- bis zur Prozessleitebene (Signal I/O bis SCADA) mit einem Werkzeug und gemeinsamer Datenbasis. Dabei entfallen große Engineering-Aufwände an den Datenschnittstellen der Systeme. Im Wasserkraftbereich kann dieser Vorteil nur sehr selten genutzt werden, da die Automatisierungs- und die Prozessleitebene unterschiedliche Erneuerungszyklen aufweisen, und somit meist nicht homogen sind. Der Prozess der Energiegewinnung und damit auch die Automatisierungsebene in Wasserkraftwerken hat sich seit geraumer Zeit nur geringfügig verändert. Der liberalisierte Energiemarkt stellt aber laufend

neue Anforderungen an SCADA-Systeme. Durch diese Umstände sind die Betreiber von großen Kraftwerkparks gezwungen, **heterogene Leittechniksysteme** zu vernetzen und zu betreiben. Des Weiteren nehmen Sicherheit und Verfügbarkeit einen sehr hohen Stellenwert ein, es wird auf eher bewährte Technik als auf neueste Trends vertraut. Daher kann man - anders als in der Industrie - die Leitsysteme von Energieversorgern als eher konservativ aufgebaut bezeichnen.

Grundsätzlich geht die Entwicklung weg von proprietären, hin zu standardisierten Kommunikationsprotokollen, Diensten, Datenbanken und Anwendungen. Es werden zunehmend Rechner und Betriebssysteme der **Office-IT** verwendet. Dies hat den Vorteil, dass der Operator mit Aussehen und der Handhabung (Look and Feel) der grafischen Benutzeroberfläche (GUI) meist schneller vertraut ist, bringt aber auch gewisse Nachteile mit sich. Aktuelle IT-Technologie hat eine sehr beschränkte Lebensdauer, da Ersatzteile aufgrund der kurzen Produktlebenszyklen nur eingeschränkt erhältlich sind. Daher sind häufige Migrationen notwendig, die ein bestimmtes Fehlerpotenzial in sich bergen. Der Einsatz von Microsoft Windows Betriebssystemen vereinfacht zwar den Datenaustausch von Produktionsinformationen zwischen SCADA- und Office-Anwendungen, bringt aber auch die Viren- und Updateproblematik mit sich. (Tauchnitz, et al., 2008 S. 199)

Durch die Integration von **Webtechnologien** werden erweiterte Kundenanforderungen wie z.B. Zugriff per Internetbrowser, Videoüberwachung, GIS[14] und MIS-Schnittstelle abgedeckt.

Als zukünftige Herausforderung von SCADA-Systemen in der Netzleittechnik kann die Integration von **Smart-Grid Technologien** betrachtet werden. Bei der Smart Grid-Technologie (intelligente Netze) kommunizieren intelligente Elektrogeräte (Verbraucher, Elektrozähler, Steuerungen usw.) mit dem Energieversorger über das Stromnetz, um z.B. eine höhere Energieeffizienz zu erreichen.

[14] GIS: Geographisches Informationssystem (z.B. digitalisierte Katasterpläne)

2.2.6 Marktübersicht

Name	Hersteller/ Verweis	Plattform	Einsatzgebiet	Merkmale
SINAUT Spectrum	Siemens / (Siemens, 2009b)	Unix	Netz- und Kraftwerksleittechnik	Java[15], X-Window[16]
Spectrum PowerCC	Siemens / (Siemens, 2009c)	Windows	Netz- und Kraftwerksleittechnik	ActiveX[17], OPC[18]
SIMATIC WinCC	Siemens / (Siemens, 2009a)	Windows	Industrie	ActiveX, OPC
iFix	GE Fanuc / (GE Fanuc, 2009)	Windows	Industrie	OPC
XA/21	GE / (GE, 2009)	Unix	Netz- und Kraftwerksleittechnik	Java, X-Window
Industrial IT 800xA	ABB / (ABB, 2009)	Windows	Industrie	OPC

Tabelle 3: SCADA Marktübersicht

[15] Java ist eine plattformunabhängige Technologie mit objektorientierter Programmiersprache. Der durch den Compiler erzeugte Bytecode ist architekturneutral. Der Bytecode wird erst bei der Ausführung durch den Just in Time Compiler (Laufzeitumgebung) in Maschinencode übersetzt und ist dadurch vom Betriebssystem unabhängig. (Victor, 2004)

[16] X-Window (auch X11 bezeichnet) ist ein Darstellungsprotokoll für Unix basierende Client-Server-Systeme. (Henning, 2004)

[17] ActiveX ist eine in Windows integrierte Schnittstellenspezifikation für Programmmodule. Sie basiert auf den OLE- und COM-Standards und wird meist bei Internet-Browsern eingesetzt. (Müller, 2004)

[18] OPC ist eine standardisierte Softwareschnittstelle nach dem Client-Server-Prinzip für die Kommunikation in Automatisierungssystemen und basierte ursprünglich auf den OLE-Standard von Microsoft. (OPC Foundation, 2009)

2.3 Kritische Infrastruktur

SCADA-Systeme werden durchwegs für die Steuerung und Überwachung von kritischer Infrastruktur eingesetzt.

Definition von kritischer Infrastruktur (KRITIS) laut BSI:

„*Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden*."(BSI, 2009a)

In folgenden kritischen Infrastrukturbereichen kommen SCADA-Systeme zum Einsatz:

- Transport und Verkehr
- Energie
- Gefahrenstoffe
- Informationstechnik und Telekommunikation
- Versorgung

Typische Einsatzbereiche sind somit die Steuerung und Überwachung von:

- Gas- Öl und Wasserpipelines
- Tunnel
- Wasserkraftwerken
- Atomkraftwerken
- Kläranlagen
- Lebensmittelindustrie
- Metallindustrie
- Raffinerien
- Autobahnen und Schnellstraßen
- Stromversorgungsnetzen
- Kalorischen Kraftwerken
- Kanalisation
- Pumpnetzwerken
- Chemische Industrie
- Papierindustrie
- Glasindustrie

Dadurch ergibt sich aus Sicht der IT-Security für viele SCADA-Systeme ein erhöhter Schutzbedarf.

3 Zwischenresümee und Präzisierung

3.1 Resümee der bisherigen Erkenntnisse

Das grundlegende Ziel der IT-Sicherheit ist der Schutz von Vertraulichkeit, Integrität und Verfügbarkeit von Informationen. Mit Hilfe von technischen, organisatorischen und personellen Maßnahmen im Rahmen eines IT-Sicherheitsmanagementsystems wird versucht, das durch verschiedene Bedrohungen entstandene Risiko auf ein akzeptables Maß zu reduzieren. Das Gesamtrisiko für ein IT-System wird dabei durch eine Risikoanalyse erfasst und bewertet. Es kann nach der detaillierten Analyse, nach dem Grundschutzansatz oder dem kombiniertem Ansatz vorgegangen werden.

Der Stand der Technik wurde in Absatz 2.1.1 beleuchtet. Durch den Einsatz von verschiedenen technischen Schutzmaßnahmen werden ein oder mehrere IT-Schutzziele sichergestellt. So wird z.B. durch Zugriffskontrollmaßnahmen die Vertraulichkeit und Integrität von Informationen geschützt. Erst durch die Kombination von verschiedenen Schutzmaßnahmen, Architekturen und Verfahren kann ein effektiver Schutz sichergestellt werden.

SCADA-Systeme sind Rechnersysteme mit denen meist dezentrale Prozesse zentral überwacht und gesteuert werden. Häufig sind diese Prozesse der kritischen Infrastruktur eines Staates oder einer Organisation zuzurechnen, wodurch der Schutzbedarf für diese Systeme erhöht ist. Anders als bei der Office-IT steht bei SCADA-Systemen die Verfügbarkeit an oberster Stelle. Die zunehmende Verschmelzung von Produktions- und Office-Netzen und der steigende Anteil von Windows-basierenden Plattformen setzen die Systeme den Gefahren der modernen IT aus. Durch das Alter und die historische Entwicklung von heute in Betrieb befindlichen SCADA-Systemen wurden IT-Sicherheitsmaßnahmen nur teilweise oder gar nicht implementiert. Die Unterstützung von partiell unsicheren Diensten, Protokollen und Methoden in aktuellen SCADA-Systemen verschärft diese Situation weiter. Moderne Systeme wie z.B. Siemens PCS7 unterstützen bereits umfassende Sicherheitskonzepte. Ältere Systeme wurden auf Grund der Kosten für Entwicklung und Migration nur weiter entwickelt ohne eine grundlegende Sicherheitskonzeption zu erhalten. Des Weiteren erfordern die zahlreichen Unterschiede zwischen Systemen der Office-IT und Produktions-IT einen behutsamen Einsatz von IT-Sicherheitskonzepten und Techniken im Umfeld von SCADA-Systemen.

3.2 Präzisierung der Aufgabenstellung

Um für das bestehende SCADA-System der Zentralwarte ein geeignetes Sicherheitskonzept zu erstellen, ist es notwendig zuvor eine Risikoanalyse für das gesamte SCADA-System durchzuführen. Dafür stehen 3 Strategien zur Verfügung, wobei für das betrachtete System nur der kombinierte Ansatz in Frage kommt, da dieser die Vorteile der beiden anderen Ansätze vereint und im Unternehmen bereits im Bereich der Office-IT eingesetzt wurde.

Beim kombinierten Ansatz wird das Gesamtsystem mindestens durch Grundschutzmaßnahmen geschützt. Nur Systemteile, die einen erhöhten Schutzbedarf aufweisen, werden einer weiteren detaillierten Risikoanalyse unterzogen. Dazu ist es nötig, die betroffenen Teile unter anderem einer Bedrohungs- und Schwachstellenanalyse zu unterziehen, um in weiterer Folge geeignete Schutzmaßnahmen zu erarbeiten. Dies ist nur mit grundlegenden Kenntnissen von Bedrohungspotenzial, Schwachstellen und Schutzmaßnahmen möglich.

Das Ziel dieser Diplomarbeit ist daher, in diesem Bereich Wissen zu erarbeiten, um durch gezieltes Aufzeigen von reell existierenden Bedrohungen, typischen Schwachstellen und deren spezifischen Lösungsansätzen ein erweitertes Sicherheitsbewusstsein beim Leser zu schaffen. Der Fokus wird dabei auf die Bedrohung durch vorsätzliche Handlungen und daraus resultierenden technischen Schutzmaßnahmen gelegt. Des Weiteren sollen IT-Schutzmaßnahmen nach dem Stand der Technik auf deren Anwendung im Umfeld von SCADA-Systemen untersucht werden, um die Grundlage für ein adäquates SCADA-Sicherheitskonzept zu bilden.

Folgende Fragen sind zu bearbeiten:

- Welchen Angreifern sind die Systeme ausgesetzt?
- Welche Angriffsmethoden werden eingesetzt?
- Wo liegt der Ursprung der Angriffe?
- Wie entwickelt sich das Bedrohungsbild?
- Wie hoch ist die Wahrscheinlichkeit eines Angriffs?
- Wurden SCADA-Systeme in der Vergangenheit bereits attackiert?
- Welche Schwachstellen besitzen SCADA-Systeme?
- Welche IT-Sicherheitsmaßnahmen werden bei SCADA-Systemen eingesetzt und was gilt es dabei zu beachten?
- Welche Standards und Richtlinien für die Sicherheit von SCADA-Systemen gibt es?

Die Hauptziele dieser Arbeit sind in folgender Mindmap grafisch dargestellt.

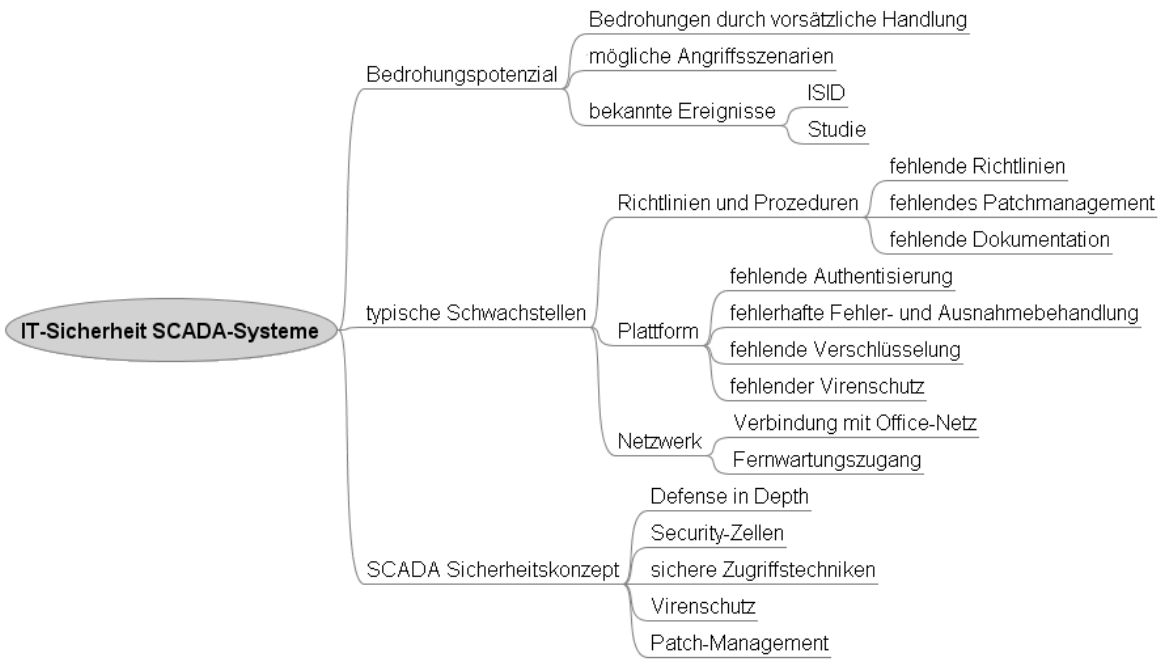

Abbildung 10: Mindmap zu IT-Sicherheitsaspekten von SCADA-Systemen

4 Bedrohungspotenzial

4.1 Bedrohungen

Wie in Absatz 2.1 beschrieben, unterteilen sich die Gefährdungen laut BSI in 5 Hauptgruppen. In dieser Arbeit soll die Gruppe der **vorsätzlichen Handlungen** genauer betrachtet werden, um ein erweitertes Sicherheitsbewusstsein zu schaffen und das Bedrohungspotenzial besser einschätzen zu können.

4.1.1 Angreifer

- **Insider**
  Insider sind meist frustrierte oder ehemalige Mitarbeiter, Lieferanten oder Geschäftspartner, die über kein besonderes Computer-Wissen verfügen, aber ihre Kenntnisse über Zielsysteme und ungeschützte Zugänge ausnützen, um Sabotage zu betreiben oder Informationen zu stehlen und zu verkaufen. (NIST SP800-82, 2008)
  Die größte Anzahl der Sicherheitsvorfälle wird durch Mitarbeiter verursacht. (BSI, 2009b)
- **Hacker**
  Hacker sind Personen, die in Computer oder Netzwerke, aus Zeitvertreib, Nervenkitzel oder um Anerkennung zu ernten, einbrechen. Ehemals waren Hacker eine kleine geschickte Gemeinschaft mit sattelfestem Computerwissen und Spezialausrüstung. Heute sind Werkzeuge, Abläufe und Protokolle im Internet frei verfügbar, deren Einsatz ist dementsprechend häufig. Hacker können in gut gesicherte Systeme meist nicht eindringen, verursachen aber häufig Ausfälle oder kurze Unterbrechungen von Diensten, die auch beachtliche finanzielle Schäden nach sich ziehen können. (NIST SP800-82, 2008)
- **Kriminelle Gruppen**
  Auf Computerkriminalität spezialisierte Gruppen attackieren Systeme, um daraus finanziellen Profit zu schlagen. Durch den Einsatz von Spam-, Phishingmethoden sowie Malware versuchen sie Identitäten zu stehlen, um damit Onlinebetrug zu begehen. Durch die Androhung einer Cyberattacke[19] versuchen sie von Unternehmen und Organisationen Geld zu erpressen. (NIST SP800-82, 2008)

[19] Cyberattacke: Ein Angriff auf IT-Systeme über das Internet

- **Phisher**

  Phisher sind Personen oder kleine Gruppen, die mit Hilfe von gefälschten Webseiten oder E-Mails an Benutzerdaten von Banken, Kreditkarten, Mail- und Online Accounts ihrer Opfer gelangen wollen, um diese gewinnbringend einzusetzen. (NIST SP800-82, 2008)
- **Spammer**

  Personen oder Organisationen die unaufgefordert E-Mails mit verstecktem oder falschem Inhalt verschicken, um Produkte zu verkaufen, Phishing zu betreiben oder Malware zu verteilen. Die bei der Spam-Abwehr entstehende Ressourcenbindung (Netzwerke, Rechner und Personen) verursacht weltweit beträchtlichen finanziellen Schaden. (NIST SP800-82, 2008)
- **Malware Autoren**

  Personen oder Organisationen, die böswillige Absichten mittels der Entwicklung und Verteilung von Malware verfolgen. Viele schädliche Viren und Würmer, wie z.B. das Melissa Makro Virus, Code Red, Loveletter, Slammer oder Blaster, haben Dateien oder ganze Festplatten beschädigt. Manche Unternehmen oder Organisationen waren durch Viren und Würmer tagelang nur teilweise handlungsfähig.(NIST SP800-82, 2008)
- **Terroristen**

  Sie versuchen kritische Infrastruktur (siehe Absatz 2.3) außer Gefecht zu setzen, zu zerstören oder auszunutzen, um die Nationale Sicherheit zu bedrohen, die Wirtschaft zu schwächen, das Vertrauen in den Staat zu brechen oder möglichst viele Menschen zu töten. Dabei reicht das Spektrum der dafür eingesetzten Mittel von Cyberwar-Strategien bis hin zu physischen Angriffen. Die terroristische Gefährdungslage sollte dem Staat und damit all seinem Bürgern so weit als möglich bekannt sein, um geeignete Gegenmaßnahmen zu treffen. (NIST SP800-82, 2008)
- **Industriespione**

  Industriespione versuchen sich das geistige Eigentum von Unternehmen unter Zuhilfenahme von verdeckten Methoden anzueignen. (NIST SP800-82, 2008)
- **Ausländische Geheimdienste**

  Ausländische Geheimdienste nutzen Cyberwerkzeuge für Spionagetätigkeiten und um Informationen zu sammeln. Einige Nationen arbeiten an der Entwicklung von Doktrinen für die Informationskriegsführung, Programmen und dazugehörigen Ressourcen. Mit solchen Ressourcen kann ein Angreifer große Schäden in Versorgungs-, Kommunikations- und Wirtschaftsinfrastrukturen bewirken und somit auch die militärische Stärke eines Landes schwächen. (NIST SP800-82, 2008)

4.1.2 Angriffsmethoden

- **Malware**

  Schadprogramme wie Viren, Würmer und Trojaner (siehe Absatz 2.1.1.2)

- **Drive-by-Downloads**

  Angreifer manipulieren meist harmlose Webseiten, um beim Browsen unbemerkt Schadcode in den Rechner des Opfers einzuschleusen. Dabei werden Sicherheitslücken im Webbrowser oder installierten Plug-ins (Erweiterungen) ausgenutzt. Die meisten Sicherheitsprobleme gibt es bei der Verwendung von Microsofts ActiveX-Elementen und JavaScript. Die Verbreitung über infizierten Webseiten steigt laut BSI rasant an und ist dabei, der führenden Verbreitung per E-Mail den Rang abzulaufen. (BSI, 2009b)

- **Exploits**

  Programme oder Kommandos, die Sicherheitslücken in Software oder Betriebssystemen ausnutzen, werden Exploits genannt. Beim Bekanntwerden einer Sicherheitslücke versucht der Entwickler der betroffenen Software in aller Regel das Problem innerhalb kürzester Zeit durch einen Patch (Korrektur) zu beseitigen. Ein Zero Day Exploit nutzt eine Schwachstelle aber innerhalb eines Tages aus, um in das System einzudringen oder Schaden anzurichten. Laut BSI steigt die Häufigkeit von Zero Day Exploits an. (BSI, 2009b)

- **DoS**

  Bei Denial of Service Attacken werden Dienste von Servern (z.B. Webserver) angegriffen und blockiert. Dies geschieht meist durch Überlastung des Systems mittels unzähliger Anfragen, damit keine weiteren Anfragen mehr bearbeitet werden können. (Meyers, et al., 2007)

- **Bot-Netze**

  Ein Bot ist ein Schadprogramm, das ferngesteuert Aktionen ausführt. Ein Bot-Netz ist die Zusammenschaltung von mit Bots infizierten Rechnern. Die Kontrolle des Bot-Netzes wird über einen oder mehrere Command-and-Control-Server erreicht. Die Kommunikation mit dem Steuerserver erfolgt meist auf der Basis von IRC (Internet Relay Chat), wobei der Trend hin zu HTTP (Hypertext Transmission Protokoll) geht. Bot-Netze werden laut BSI für den Versand von Spam, Aufzeichnung von Tastaturanschlägen (Keylogging) und Durchführung von verteilten DoS-Angriffen (DDoS) eingesetzt. (BSI, 2009b)

4.1.3 Bedrohungsursprung

Das British Columbia Institute of Technologie (BCIT) betreibt die sogenannte Industrial Security Incident Database (ISID). Diese Datenbank zeichnet IT-Sicherheitsereignisse auf, die industrielle Kontroll- und Prozesssysteme betreffen. Der Eintrag eines Vorfalls erfolgt bei öffentlichem Bekanntwerden oder freiwillig durch die betroffenen Unternehmen.

Eine Studie des BCIT aus dem Jahre 2004 (BCIT, 2004) zeigt die Verschiebung der Sicherheitsereignisse weg von **internen** hin zu **externen Angriffen**.

Bei Vergleich von Abbildung 11 und Abbildung 12 aus der ISID zeigt sich ein Anstieg der externen Angriffe von 31% auf 70% innerhalb von nur 3 Jahren.

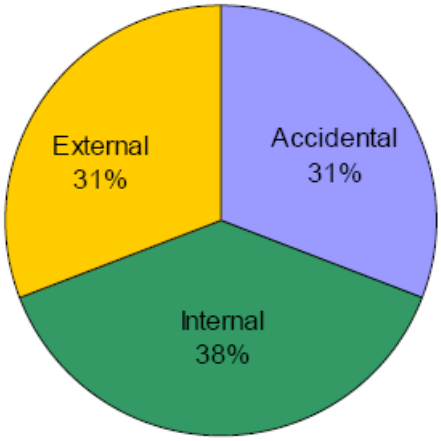

Abbildung 11: Sicherheitsereignisse (1982-2000) (BCIT, 2004)

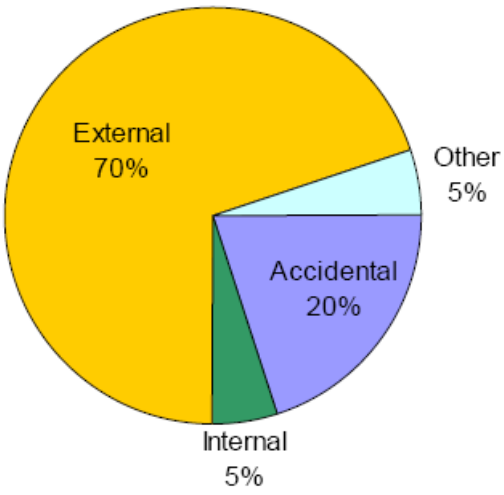

Abbildung 12: Sicherheitsereignisse (2001-2003) (BCIT, 2004)

Die Autoren der BCIT-Studie geben als mögliche Ursachen mehrere Gründe an:

- Das Auftauchen der ersten **automatisierten Attacke** mit dem Wurm „Code Red“ im Juli 2001 zeigt, dass mittlerweile viele Attacken automatisiert ablaufen und nicht zielgerichtet sind. SCADA-Systeme sind eher zufällig als absichtlich zum Ziel geworden.
- Die zunehmende Verwendung von **gebräuchlichen Betriebssystemen** (z.B. Windows und Linux) und **Anwendungen** (z.B. SQL-Server) im Bereich von HMI, Engineering-Plätzen und Archiv-Systemen (Historian Systems) schafft Angriffsflächen. Diese Systeme sind oft nach Business-Anforderungen konfiguriert und sind für eine Vielzahl von Viren und Angriffen anfällig. Die Kosten für das Patch-Management solcher Systeme verschärfen das Problem.
- Die **fortschreitende Vernetzung** der Systeme hat Abhängigkeiten und Verwundbarkeit geschaffen, die zu wenig berücksichtigt wurden.

Die relativ große Veränderung des Bedrohungsbildes in kurzer Zeit sollte die Sicherheitsverantwortlichen mahnen, ihre Risikoanalysen und Sicherheitsrichtlinien in überschaubaren Zeitabständen zu überdenken und an veränderte Bedrohungslagen anzupassen. IT-Sicherheit ist nicht allein durch Einmalmaßnahmen zu erreichen, sondern sie ist vielmehr ein kontinuierlicher Prozess.

In weiterer Folge wurde der exakte Eintrittspunkt genauer untersucht, um das Bedrohungsbild klarer darzustellen:

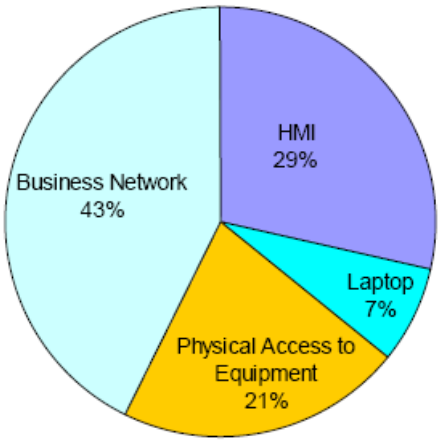

Abbildung 13: Interne Sicherheitsereignisse (BCIT, 2004)

Das Büro-Netzwerk stellt das größte Bedrohungspotenzial bei den internen Ereignissen dar. Nicht umsonst wird in vielen Dokumenten die strikte Trennung der Netze oder der Einsatz von gut gewarteten Firewalls empfohlen. Auch der physische Schutz einer Anlage sollte nicht vernachlässigt werden.

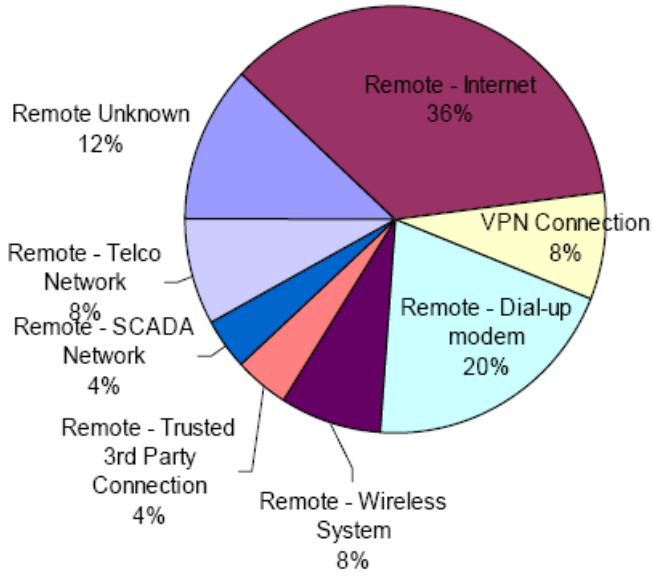

Abbildung 14: Externe Sicherheitsereignisse (BCIT, 2004)

Bei den Ereignissen mit externem Ausgangspunkt führt das Internet mit gut 1/3 der Vorfälle. Remotezugänge mit Modem- und VPN-Verbindungen stellen die nächst größere Gruppe dar. Die Anzahl der Vorfälle mit Wireless-Zugang dürfte durch die wachsende Verbreitung in Zukunft weiter zunehmen. Insgesamt kann man sagen, dass es sehr viele Wege und Möglichkeiten gibt, um in ein Netzwerk einzudringen. Es reicht nicht aus, die Sicherheitsanstrengungen auf einen Zugangspunkt zu konzentrieren (Stichwort Internetfirewall), weil dabei viele andere Zugangswege außer acht gelassen werden und das Restrisiko für die Anlage beträchtlich bleibt.

4.1.4 Bedrohungsentwicklung

Das BSI veröffentlicht den Lagebericht zur IT-Sicherheit in Deutschland. Der Bericht gibt einen Überblick über aktuelle Schwachstellen, Bedrohungen, Angriffsmöglichkeiten, Trendtrends und Aktivitäten. Das BSI versucht auf der Basis von Recherchen fundierte Entwicklungsprognosen abzugeben.

„Einige Angriffsmethoden werden bei Internetkriminellen immer beliebter, während andere an Bedeutung verlieren. Fakt ist, dass Tag für Tag Tausende neue Schadprogramme das Internet überschwemmen. Hinzu kommen neue Technologien, deren Risikopotenzial heute zwar schwer abschätzbar ist, jedoch mit zunehmender Verbreitung und Akzeptanz vermutlich steigen wird.“ (BSI, 2009b)

In Abbildung 15 ist die Entwicklung der Gefährdungen inklusive Prognose dargestellt.

Abbildung 15: Gefährdungstrends (BSI, 2009b)

In Abbildung 16 zeigt das BSI Risikoentwicklung und –prognose für ausgewählte Anwendungen.

Technologie / Anwendung	2007	2009	Prognose
Voice over IP	↑	→	→
Mobile Datenübertragung	—	↑	↑
Web 2.0	—	↑	↑
SCADA	→	↑	↑
DNS	—	↑	↑
Multifunktionsgeräte	—	↑	→
Schnittstellen und Speichermedien	—	↑	→
Netzkoppelelemente	—	↑	↑
SOA	—	↑	↑

↑ Gefährdung nimmt zu → gleichbleibende Gefährdung ↓ Gefährdung sinkt

Abbildung 16: Risikopotenzial für Angriffsmöglichkeiten in ausgewählten Anwendungen und Technologien (BSI, 2009b)

Das Risiko für SCADA-Systeme wird laut BSI weiter steigen.

Der Lagebericht (BSI, 2009b) stellt fest, dass die Hersteller und auch Nutzer von SCADA-Systemen sich der Gefahrensituation zunehmend bewusst werden. Die besonderen Sicherheitsanforderungen dieser Systeme fließen nach und nach in Normen und Empfehlungen ein. Heute vertriebene und in Betrieb befindliche Systeme sind aber oftmals noch nicht ausreichend geschützt. Laut Bericht wurden 2003 mehrere Schwachstellen aufgedeckt, wobei zwei in stark verbreiteten Softwareprodukten zur Kontrolle von SCADA-Systemen gefunden wurden.

„Wegen einer fehlerhaften Systemarchitektur führte in den USA ein Softwareupdate in einem Kernkraftwerk zu einem ungeplanten 48-stündigen Ausfall des Werks, weil das Prozesssteuerungssystem durch das Softwareupdate im Bürokommunikationsnetz gestört wurde.“(BSI, 2009b) *(Details siehe Absatz 4.3.2, „Hatch Atomkraftwerk 2008“)*

4.1.5 Eintrittswahrscheinlichkeit

Das Idaho National Laboratory (INL) ist eine wissenschaftliche Einrichtung, die das Department of Energy (DOE) der USA unterstützt. Das vom INL betriebene „National SCADA Test Bed Program" (NSTB) beschäftigt sich mit Sicherheitsbelangen von SCADA-Systemen in der Energiewirtschaft. (INL, 2009)

In Abbildung 17 sind Eintrittswahrscheinlichkeit, Auswirkung und Angriffsmethoden laut NSTB dargestellt. Dabei werden die Angreifer und deren Angriffsmethoden in drei Gruppen (GRPI-III) eingeteilt.

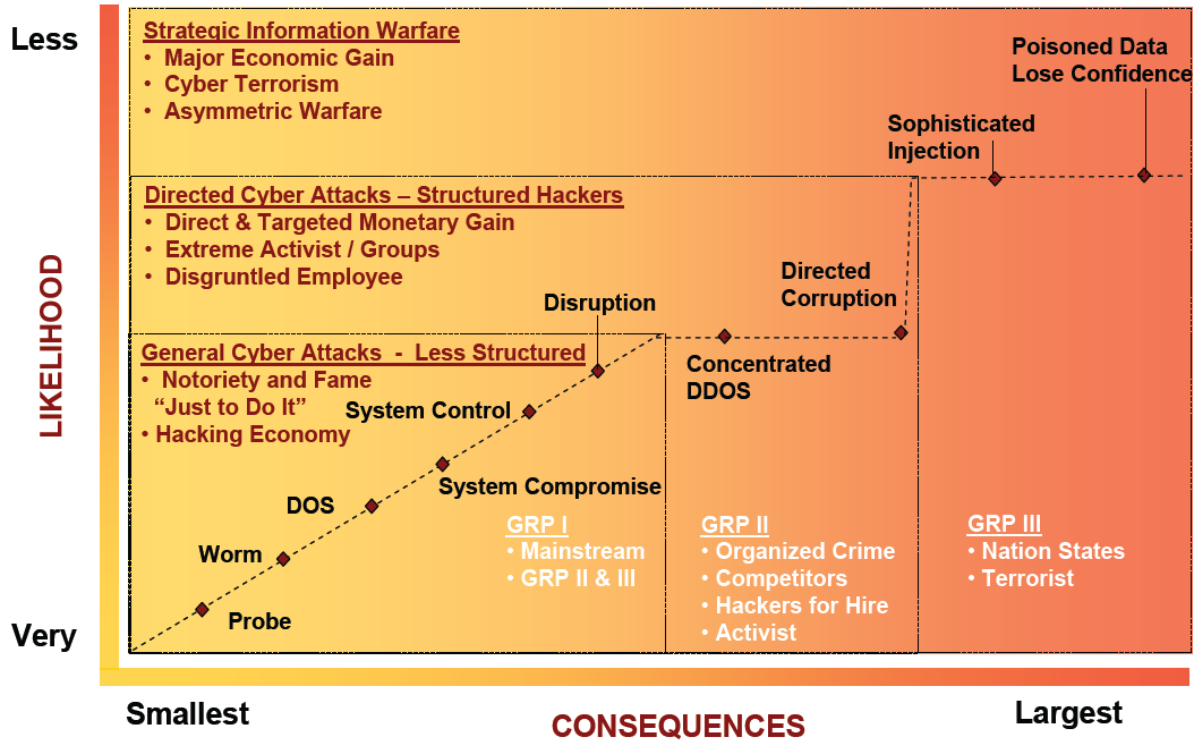

Abbildung 17: Eintrittswahrscheinlichkeit und Auswirkungen von Angriffsmethoden (INL, 2007)

- **Angreifer Gruppe 1 (GRP I)**
  Allgemein übliche Angriffsmethoden, einzelne Angreifer, Angriffswahrscheinlichkeit ist sehr hoch bis mittel, Auswirkungen gering bis mittel

- **Angreifer Gruppe 2 (GRP II)**
  Zielgerichtete Angriffsmethoden, Insider, organisierte Hacker oder kriminelle Gruppen, Angriffswahrscheinlichkeit mittel, Auswirkungen mittel bis hoch

- **Angreifer Gruppe 3 (GRP III)**
  Strategische IT-Kriegsführung, Ausländische Geheimdienste oder Staaten, Angriffswahrscheinlichkeit gering, Auswirkungen hoch bis sehr hoch

4.2 Mögliche Angriffsszenarien

Es gibt eine Vielzahl von möglichen Angriffsszenarien. Die hier angeführten stammen aus einer Studie des United States General Accounting Office aus dem Jahr 2004, die für den Kongress der Vereinigten Staaten angefertigt wurde. (GOA, 2004)

- Beeinträchtigung des SCADA-Betriebes durch das Blockieren oder Verzögern des Datenflusses durch das Prozess- oder Office-Netz.
- Nicht autorisierte Programmänderungen in SPS, PLS und SCADA-Systemen, Manipulation von Grenzwerten, nicht autorisierte Befehlsgabe mit dem Risiko von Beschädigung oder Ausfall der Produktionsanlage oder Produkten, Schäden an der Umwelt, Beeinträchtigung oder Ausfall von kritischer Infrastruktur.
- Senden von falschen Prozessinformationen um nicht autorisierte Änderungen zu verschleiern oder unangebrachte Bedienhandlungen des Operators zu provozieren.
- Ändern der PLS-Software oder -Einstellungen um unvorhergesehene Ergebnisse zu produzieren.
- Einschleusen von Malware, um den Betrieb zu stören oder zum Erliegen zu bringen.
- Ändern von Rezepten oder Arbeitsabläufen um Produkte, Anlagen oder Personen zu schädigen.

Des Weiteren sind Systeme mit großer geografische Ausdehnung und unbesetzten Substationen der Gefahr eines unbemerkten Einbruches ausgesetzt. Der Angreifer könnte eine bedrohliche Verbindung in das Kontrollzentrum aufbauen.

4.3 Bekannte sicherheitsrelevante Ereignisse

Sicherheitsrelevante Ereignisse werden meist nur dann öffentlich bekannt, wenn die Auswirkungen auch öffentlich spürbar wurden. Die meisten Unternehmen oder Organisationen verschweigen solche Ereignisse aus Imagegründen. Laut Schätzungen des Idaho National Laboratory kommen auf ein in der Industrial Security Incident Database (siehe Absatz 4.1.3) gemeldetes Sicherheitsereignis 100 bis 400 ungemeldete Vorfälle. (INL, 2007)

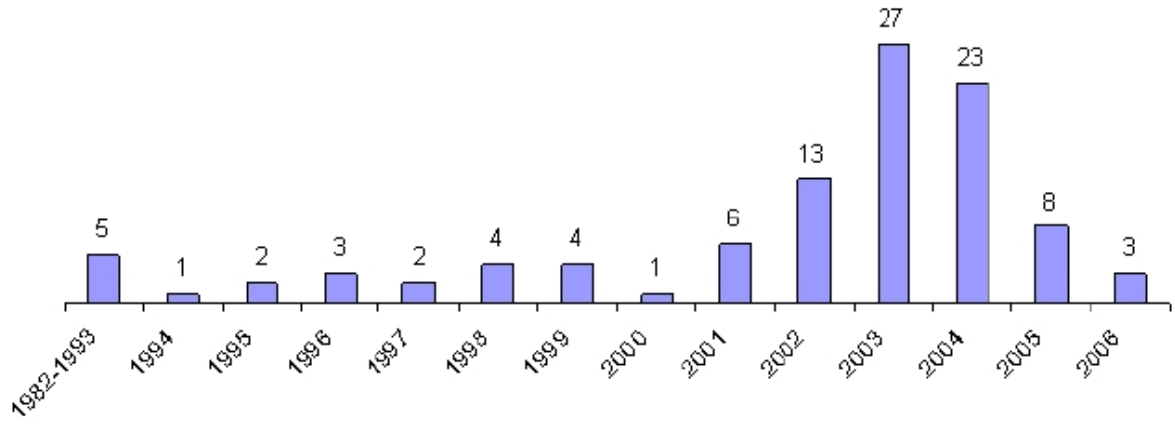

Abbildung 18: Jährlich gemeldete sicherheitsrelevante Ereignisse in der ISID

In Abbildung 18 sind alle bis Juni 2006 in der ISID registrierten und validierten Ereignisse nach Eintragsjahr dargestellt. Markant ist der sehr starke Anstieg um das Jahr 2003. Dieser ist laut INL (INL, 2007) wahrscheinlich durch den unbedarften Einsatz neuer Technologien, wie z.B. Internet und zunehmender Verbindungen mit dem Office-Netz der Unternehmen, begründbar. Die Implementierung von Sicherheitsmaßnahmen in industriellen Steuerungssystemen hat dieser Entwicklung anscheinend entgegengewirkt.

4.3.1 Angriffe

- **Worcester Airport 1997**

  Im März 1997 hat ein Jugendlicher aus Worcester (Massachusetts, USA) Teile des öffentlichen Telefonnetzes über ein mit dem Telefonsystem verbundenes Service-Modem lahm gelegt. Dadurch war das Telefonsystem des Kontrollturmes, der Flughafensicherheit, der Flughafenfeuerwehr und des Wetterdienstes außer Betrieb. Des Weiteren war die Hauptfunkstation des Kontrollturmes, eine Funkstation für die Aktivierung der Landebahnbefeuerung und der Drucker für die Protokollierung der Flugbewegungen außer Betrieb. In der nahe gelegenen Stadt Rutland waren weitere 600 private und kommerzielle Telefonanschlüsse ausgefallen. (CNN, 1998)

- **Maroochy Shire Abwassermanagement 2000**

  Im Frühjahr 2000 bewarb sich ein ehemaliger Angestellter einer Firma, die Abwassermanagementsysteme entwickelt, bei einer australischen Gemeinde, die ein solches System geliefert bekam. Der Mann wurde aber abgewiesen. Aus Rache darüber hat er über eine Dauer von 2 Monaten in mindestens 46 Fällen das Abwassermanagementsystem dieser Gemeinde (Maroochy Shire) gehackt. Die Polizei fand in seinem Auto Funk- und Computerequipment mit dem er die Angriffe ausführte. Durch die Angriffe wurden insgesamt mehrere Millionen Liter ungeklärtes Abwasser in Flüsse, Parks und in ein Hotel geleitet. (The Register, 2001)

- **Georgien-Konflikt 2008**

  Beim Georgien-Konflikt zwischen Russland und Georgien im Herbst 2008 waren georgische Netzwerke starken DoS-Angriffen ausgesetzt. Regierungs- und Nachrichtenwebseiten waren nicht erreichbar oder bauten sich nur sehr langsam auf. Internetserver waren teilweise unter fremde Kontrolle geraten, in Blogs wurde darauf hingewiesen, dass der Inhalt von offiziellen georgischen Websites momentan gefälscht sein könnte. (Der Standard, 2009)

4.3.2 Unbeabsichtigte Auswirkungen

- **Northeast Power Blackout 2003**

  Am 14. August 2003 führte ein Programmfehler im Alarmierungssystem des SCADA-Systems XA/21 von General Electric beim Energieversorger FirstEnergy (USA) dazu, dass sich die Operatoren der Leitzentrale der gefährlichen Situation bei von ihnen getätigten Schalthandlungen nicht bewusst waren. Zusätzlich war die Übersicht über verfügbare Netzkapazitäten beeinträchtigt, da die automatisierte Netzzustandserkennung (State Estimation) der nordamerikanischen Netzregion Midwest mit unvollständigen Netztopologie-Änderungen versorgt wurde und somit auch die Netzsicherheitsanalyse (Contingency Analysis) fehlerbehaftet war. Der Ausgangspunkt des Netzausfalls war die Unterbrechung mehrerer wichtiger 345kV Leitungen in Norden von Ohio wegen Erdschlüssen mit Bäumen. Dies hat möglicherweise zu kaskadierten Überlastungen in 345kV und 138kV Leitungen geführt, die wiederum zu einem großflächigen Netzausfall führten. Von diesem Stromausfall waren 50 Millionen Menschen im Norden der USA bis zu 4 Tage lang betroffen. Insgesamt fiel eine Leistung von 61.800MW, bestehend aus 508 Generatoren in 256 Kraftwerken, aus. Der gesamte volkswirtschaftliche Schaden dieses Ereignisses beläuft sich laut Schätzungen auf 4 bis 10 Milliarden US-Dollar. (U.S.-Canada Power System Outage Task Force, 2004)

- **Davis-Besse Atomkraftwerk 2003**

  Im August 2003 hat die Atomregulierungsbehörde der USA bestätigt, dass der „Slammer"-Wurm[20] am 25. Jänner 2003 in das Netz des Davis-Besse Atomkraftwerks eingedrungen ist und ein Sicherheitsüberwachungssystem für fast 5 Stunden ausfallen lies. Der Wurm drang über eine Lieferanten-Verbindung ein, die an der Firewall des Kraftwerkes vorbei führte. Die umgangene Firewall war gut konfiguriert und hätte das Eindringen des Wurms durch Blockieren des UDP-Ports 1434 verhindert. Glücklicherweise war das Kraftwerk für Instandsetzungsarbeiten außer Betrieb. Des Weiteren existierte für das ausgefallene Sicherheitsüberwachungssystem ein redundantes analoges System, das nicht betroffen war. (SecurityFocus, 2003)

[20] „Slammer" ist ein Wurm der ungepatchte Microsoft SQL-Server befällt. Der Wurm trat am 25.Jänner 2003 zum ersten Mal auf und infizierte innerhalb von 30 Minuten 75.000 ungepatchte SQL-Server. Als Folge brach das Internet für mehr als 4 Stunden fast vollständig zusammen, da viele DNS-Server ausfielen oder nur eingeschränkt arbeiteten. (TecChannel, 2003)

- **Hatch Atomkraftwerk 2008**

  Als ein Techniker im März 2008 ein Softwareupdate auf einem Rechner im Office-Netzwerk des Atomkraftwerks Hatch in den USA installierte und diesen neu startete, wurde das Kraftwerk vom Sicherheitssystem automatisch heruntergefahren. Der Rechner synchronisierte sich mit dem primären Kontrollsystem des AKWs und setzte dabei einige Daten zurück. Das Kontrollsystem interpretierte das als Abfall des Kühlwasserniveaus und schaltete Block 2 ab. Dem Techniker war zwar bewusst, dass der Rechner mit dem Kontrollsystem kommuniziert, aber nicht, dass Daten in Richtung Prozess geschrieben wurden. (The Washington Post, 2008)

4.3.3 Unbeabsichtigte Auswirkungen durch IT-Sicherheit

- **Netzwerkscan**

  Während eines Ping-Durchlaufes[21] in einem aktiven SCADA-Netz, das Roboterarme steuert, wurde beobachtet, dass ein Arm aktiv wurde und sich um 180° drehte. Der Controller des Roboters war vor dem Ping-Durchlauf im Standby-Modus. Glücklicherweise war die im Raum anwesende Person außerhalb der Reichweite des Armes.

  Bei einem ähnlichen Vorfall legte ein Ping-Durchlauf in einem Prozess-Netz für die Produktion von integrierten Schaltkreisen (ICs) einen Controller lahm. Der eigentliche Zweck des Ping-Durchlaufes war die Inventarisierung aller Netzwerkhosts. Bei dem Unfall wurden Halbleiter-Wafer im Wert von 50.000 US-Dollar zerstört. (Sandia National Laboratories, 2005)

- **Penetrationstest**

  Ein Erdgasversorger beauftragte ein IT-Unternehmen für Sicherheitsberatung mit der Durchführung eines Penetrationstestes im Office-Netzwerk. Die Berater wagten sich unvorsichtigerweise in einen Teil des Netzes, der direkt mit dem SCADA-System verbunden war. Der Penetrationstest blockierte das SCADA-System soweit, dass der Gasversorger 4 Stunden lang kein Gas durch seine Pipelines schicken konnte. (Sandia National Laboratories, 2005)

[21] Ping ist ein Programm, das durch das Senden von Echo-Request-Paketen über ICMP die Erreichbarkeit von Hosts in einem Netzwerk prüft. Durch die Zeitdifferenz des gesendeten und empfangenen Paketes wird zusätzlich die Laufzeit berechnet. Bei einem Ping-Durchlauf in einem Subnetz wird an jede mögliche Hostadresse ein Ping geschickt, um vorhandene Hosts zu entdecken. Ping ist nach dem Internetstandard RFC 1574 definiert.

5 Typische Schwachstellen

Die Richtlinie für Sicherheit von industriellen Steuerungssystemen[22] (NIST SP800-82, 2008) teilt potenzielle Schwachstellen in die 3 Kategorien **Richtlinien und Prozeduren, Plattform** und **Netzwerk** ein.

5.1.1 Mangelhafte Richtlinien und Prozeduren

Schwachstellen entstehen häufig durch unvollständige, unangemessen oder gar fehlende Sicherheitsrichtlinien, Dokumentationen und Implementierungsprozeduren.

Häufige Schwachstellen in den Richtlinien und Prozeduren laut NIST sind:

- **Mangelhafte Sicherheitsrichtlinie**
  Schwachstellen entstehen durch unvollständige, mangelhafte oder fehlende Regelungen.
- **Fehlendes Sicherheitstraining und Sicherheitsbewusstseinsbildung**
  Mitarbeiter handeln oft aus Unwissenheit fahrlässig. Sicherheitsrichtlinien, Standards und sichere Arbeitsweisen sollten von Zeit zu Zeit ins Bewusstsein gerufen werden.
- **Mangelhafte Sicherheitsarchitektur und –design**
  Automatisierungsingenieure haben aus historischen Gründen meist keine oder nur unzureichende Ausbildung in IT-Sicherheit. Hersteller implementieren erst seit überschaubarer Zeit Sicherheitsfunktionen in die Systeme.
- **Fehlende Entwicklung oder Dokumentation von speziellen Sicherheitsprozeduren in der Sicherheitsrichtlinie**
  Speziell notwendige Sicherheitsprozeduren müssen entwickelt, dokumentiert und trainiert werden.
- **Fehlende Richtlinien für Geräteimplementierung**
  Richtlinien müssen gepflegt und leicht zugänglich sein, um im Störungsfall (Gerätetausch) richtig handeln zu können.
- **Mangelnde organisatorische Regelungen**
  Meist fehlt der Einsatz von Sicherheitsverantwortlichen in der Prozessleittechnik.
- **Fehlende Sicherheitsaudits**
  Externe Auditoren sollten die Anlage regelmäßig untersuchen und die Einhaltung der Sicherheitsrichtlinie kontrollieren, sowie auf neue Entwicklungen hinweisen.

[22] Als industrielle Steuerungssysteme werden SCADA-Systeme, Prozessleitsysteme und Speicherprogrammierbare Steuerungen bezeichnet.

- **Kein SCADA spezifischer Disaster Recovery Plan**
  Ein geeigneter Notfallplan reduziert die Ausfallszeit beim Ausfall von wichtigen Systemkomponenten oder Anlagen.
- **Mangelhaftes Change Management**
  Fehlende Prozeduren zur Durchführung und Dokumentation von Hard-, Software- und Konfigurationsänderungen gefährden den sicheren Betrieb.

5.1.2 Plattform-Schwachstellen

Laut NIST (NIST SP800-82, 2008) haben Sicherheitslücken in der Plattform ihren Ursprung in Nachlässigkeit, Fehlkonfiguration und schlechter Wartung von Betriebssystem, Hardware und Anwendungen. Diese Schwachstellen können durch das Patchen von Betriebssystem und Anwendungen, dem Einsatz von Zugriffskontrollmaßnahmen und Virenschutz vermieden werden.

5.1.2.1 Konfiguration

- **Patch-Management**
  Aktuelle Sicherheitspatches für Betriebssystem und Anwendungen sind nicht installiert oder wurden vor der Implementierung nicht ausreichend getestet.
- **Default-Konfiguration**
  Verwundbare Dienste, Ports und Anwendungen laufen ohne Notwendigkeit.
- **Konfigurationen nicht gespeichert oder gesichert**
  Konfigurationen sind nicht dauerhaft (bootresistent) gespeichert oder es ist kein aktuelles Backup abgelegt.
- **Passwort**
  keine Passwortrichtlinie, fehlende Anwendung von System-, Anwendungs- oder Bildschirmschonerpasswort, Verwendung schwacher Passwörter, notieren des Passwortes auf Monitor oder Tastatur, Verwendung von Gruppen-Passwörtern, verwenden von herstellerseitigen Default-Passwörtern, kein Passwortwechsel
- **Mangelhafte Benutzerrechte**
  zu wenig oder zu viele Rechte, schlecht konfigurierte oder fehlende Benutzer-Rollen-Verwaltung, zu wenig Rechte, um im Störungsfall Gegenmaßnahmen treffen zu können, zu viele Rechte (privilegierte Rechte oder Administratorenrechte) am Betriebssystem

5.1.2.2 Hardware

- **Mangelnder physischer Zugriffsschutz**
  Zugang zur Leitstelle, Rechnerräumen, Sicherungsmedien, Kommunikations- und Übertragungseinrichtung, Steuerschränken im Freien usw. ist nur mangelhaft oder nicht gesichert. Es existieren keine Aufzeichnungen über Zutritt bzw. keine Videoüberwachung für hochsensible Bereiche.

- **Unsichere Fernzugänge**
  Einsatz von Wartungsmodems ohne Sicherheitsmaßnahmen, fehlende Richtlinien und Dokumentation
- **Multi-Homed-Hosts**
  Rechner, die in mehren Netzwerken eingebunden sind und Daten ohne Beschränkungen von einem in das andere Netz routen
- **Nicht dokumentierte Geräte**
  unkontrollierter Zugang über nicht dokumentierte Geräte wie z.B. Wartungsmodems
- **Technische Mängel**
  mangelhafte Stromversorgung, Klimatisierung und Redundanzkonzepte

5.1.2.3 Software

- **Nichtbenötigte Dienste laufen**
  Es besteht die Gefahr, dass Dienste missbraucht oder Schwachstellen in Diensten ausgenutzt werden. System-Hardening durchführen (unnötige Dienste deaktivieren)
- **Mangelhafte Fehler- und Ausnahmebehandlung**
  schlecht programmierte Dienste und Anwendungen
- **Verwendung unsicherer Dienste, Applikationen**
  fehlende Verschlüsselung oder Authentisierungsmaßnahmen, Verwendung von unsicheren Diensten wie OPC (OLE for Process Control), ftp, telnet
- **Verwendung unsicherer Kommunikationsprotokolle**
  DNP 3.0, Modbus, Profibus und einige andere offene Protokolle sind in vielen industriellen Anwendungen Standard, obwohl sie wenige oder keine Sicherheitsfunktionen unterstützen.
- **Standardmäßig deaktivierte Sicherheitsfunktionen**
  Vorhandene Sicherheitsfunktionen in SCADA-Systemen sind oft nicht standardmäßig aktiviert.
- **Mangelhafter Zugriffsschutz auf Konfigurations- und Programmiersoftware**
  Operatoren können bei fehlerhafter Konfiguration mit ihrem Benutzerkonto Konfigurationen oder Programme ändern.
- **Fehlender Einsatz von IDS/IPS-Software**
  Ohne IDS/IPS-Systeme erfolgt keine oder zu späte Alarmierung beim Eintritt von Sicherheitsereignissen. IDS/IPS-Systeme müssen auf korrekte Funktion mit dem SCADA-System getestet werden, um den ordnungsgemäßen Betrieb nicht zu beeinträchtigen.

- **Fehlende oder nicht gewartete Logdateien**
  Die Nachvollziehbarkeit von Eingriffen und Störungen ist ohne entsprechende Protokollierung nicht möglich.
- **Fehlender oder mangelhafter Malwareschutz**
  Schwachstellen entstehen durch nicht aktuellen oder fehlenden Malwareschutz, der nicht oder unzureichend auf dem Zielsystem getestet oder vom Hersteller nicht freigegeben wurde. Auf die besonderen Anforderungen (Verfügbarkeit und Performance) sind bei der Auswahl und Betrieb von Malwareschutz Rücksicht zu nehmen.

5.1.3 Netzwerk-Schwachstellen

Schwachstellen entstehen laut NIST (NIST SP800-82, 2008) durch Fehler, Fehlkonfigurationen, schlechter Administration und unkontrollierte Verbindung von Netzen. Dies kann durch den Einsatz von verschiedenen Sicherheitsmaßnahmen wie Netzwerkdesign, Verschlüsselung der Übertragung, Einschränkung des Netzwerkverkehrs und physischen Schutz des Netzwerkes vermieden werden.

5.1.3.1 Konfiguration

- **Schwache Netzwerk-Sicherheitsarchitektur**
  Netzwerke werden oft nach Geschäfts- und Betriebsanforderungen erweitert, ohne auf die Sicherheit Rücksicht zu nehmen.
- **Fehlende Einschränkungen des Gerätezugriffs**
  Oft besteht keine Einschränkung, welche Personen oder Geräte auf Netzwerkkomponenten zugreifen dürfen. Der Einsatz von Access Control Lists (ACL) wird empfohlen.
- **Schlecht konfigurierte Sicherheitseinrichtungen**
  ungenau konfigurierte Firewalls oder Router-ACLs, Einsatz von Standardparametern, offene Ports, aktivierte anfällige Netzwerkdienste, die nicht benötigt werden
- **Konfigurationen nicht gespeichert oder gesichert**
  Konfigurationen sind nicht dauerhaft (bootresistent) gespeichert oder es ist kein aktuelles Backup abgelegt. Der Einsatz von Parametrieranweisungen wird befürwortet.
- **Übertragung von Passwörtern in Klartext**
  Passwörter für den Zugang zu Netzwerkkomponenten werden oft in Klartext übertragen. Der Einsatz von verschlüsselten Kommunikationsmethoden (SSH, https usw.) wird empfohlen.
- **Passwörter werden nie geändert**
  Passwörter von Netzwerkkomponenten sollten regelmäßig geändert werden.

- **Fehlender oder mangelhafter Zugangsschutz**
  fehlender Passwortschutz, Verwendung von Default-Passwörtern des Herstellers

5.1.3.2 Hardware

- **Mangelnder physischer Zugriffsschutz**
  Der Zugang zu Netzwerkkomponenten, Kommunikations- und Übertragungseinrichtung ist nur mangelhaft oder gar nicht gesichert. Es gibt keine Aufzeichnungen über Zutritt bzw. keine Videoüberwachung für hochsensible Bereiche. Der Zutritt sollte nur für autorisiertes Personal möglich sein.
- **Ungesicherte physische Ports**
  Über USB- und PS/2-Ports können Schadsoftware eingeschleust oder Informationen abgezogen werden.
- **Technische Mängel**
  mangelhafte Stromversorgung, fehlende Klimatisierung und Redundanzkonzepte

5.1.3.3 Perimeter

- **Security-Zellen nicht definiert**
  nicht autorisierter Zugriff auf Prozessnetze möglich, kein sicherer Datenaustausch, keine definierte sichere Schnittstelle
- **Keine oder mangelhaft konfigurierte Firewalls**
  Schlecht konfigurierte Firewalls erlauben unzulässigen Datenverkehr zwischen Netzen. Es besteht die Gefahr von Malwareverbreitung über Netzwerksgrenzen und nicht autorisierten Zugriff auf sensible Informationen.
- **Mischung von Netzwerkverkehr**
  Der Netzwerkverkehr von Automatisierungssystemen stellt verstärkte Anforderungen an Determinismus und Verfügbarkeit. Fremder Verkehr könnte zu viele Ressourcen belegen.
- **Dienste des SCADA-Netzwerkes außerhalb des Produktionsnetzes**
  DNS- und DHCP-Server des SCADA-Systems sind häufig in Office-IT-Netzen angesiedelt. So wird das Prozess-Netz vom Office-Netz, das ein anderes Verfügbarkeits- und Zuverlässigkeitsniveau aufweist, abhängig.

5.1.3.4 Überwachung und Erfassung

- **Unangemessene Firewall und Router Logs**
  Ohne angemessene Logs ist die Analyse von Sicherheitsereignissen nicht möglich.

- **Keine Netzwerküberwachung**
  Ohne Überwachung ist es möglich, dass Ereignisse nicht entdeckt werden und größerer Schaden eintritt, Fehler und Fehlkonfigurationen bleiben dadurch unerkannt.

5.1.3.5 Übertragung

- **Mangelnde Netzwerkdokumentation**
  Undokumentierte Verbindungen werden nicht in das Sicherheitskonzept einbezogen und stellen somit ein großes Sicherheitsrisiko dar.
- **Verwendung von Standardprotokollen im Klartext**
  Netzwerkaktivitäten können mit frei verfügbarer Protokollanalyse-Software abgehört oder manipuliert werden. Verwendung von sicheren Übertragungstunneln oder verschlüsselten Protokollen wird empfohlen.
- **Fehlende oder mangelhafte User- und Geräteauthentisierung**
  Viele Kommunikationsprotokolle unterstützen keine oder nur schwache Authentisierungsmethoden, dadurch wird das Mithören und Wiedergeben (Replay) von Netzwerkverkehr erleichtert.
- **Mangelnde Integritätsüberwachung**
  Durch das Fehlen von integritätssichernden Maßnahmen in den meisten Protokollen kann Netzwerkverkehr unbemerkt manipuliert werden. Der Einsatz von Lower Layer Protocols (Protokolle der OSI-Schicht 1-4) mit Integritätsschutz, wie z.B. IPsec, kann diese Bedrohung ausschalten.

5.1.3.6 Drahtlose Kommunikation

- **Unzureichende Authentisierung zwischen Client und Access-Point**
  Starke gegenseitige Authentisierung zwischen Client und Access-Point ist notwendig, um sicherzustellen, dass Clients sich nicht mit Access-Points von Angreifern verbinden und Angreifern der Zugang zum Wireless-LAN verwehrt bleibt.
- **Unzureichende Verschlüsselung zwischen Client und Access-Point**
  Daten müssen ausreichend stark verschlüsselt sein, um nicht mitgehört zu werden. Die WEP-Verschlüsselung in Wireless-LANs gilt als mittlerweile unsicher, da sie relativ leicht entschlüsselt werden kann. Der Einsatz des neueren WPA2-Verfahrens wird empfohlen, da dieses bislang als sicher gilt. (Meyers, et al., 2007 S. 254)

6 Sicherheitskonzepte und Schutzmaßnahmen

Um SCADA-Systeme vor Bedrohungen und Angriffsmethoden zu schützen, gibt es eine Reihe von Verteidigungsstrategien und daraus resultierenden Maßnahmen. Bei der Konzeption und Implementierung ist darauf zu achten, dass den besonderen Erfordernissen von Produktionssystemen Rechnung getragen wird.

In der Special Publication 800-82 „Guide to Industrial Control Systems (ICS) Security“ (NIST SP800-82, 2008) werden die in der Special Publication 800-53 „Recommended Security Controls for Federal Information Systems and Organizations” (NIST SP800-53, 2009) allgemein definierten Schutzmaßnahmenfamilien (siehe Tabelle 4) für industrielle Steuerungssysteme spezifiziert.

IDENTIFIER	FAMILY	CLASS
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Certification, Accreditation, and Security Assessments	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational

Tabelle 4: Organisation von IT-Schutzmaßnahmen (NIST SP800-53, 2009)

Die Schutzmaßnahmen werden dabei in 17 Familien unterteilt, die den 3 Klassen Technik, Betrieb und Management zugeordnet werden.

In weiterer Folge werden einige daraus abgeleitete technische Maßnahmen näher erläutert.

6.1 Tiefgestaffelte Verteidigung

Der ANSI-Standard[23] der International Society of Automation (ISA) definiert den Begriff tiefgestaffelte Verteidigung (Defence in Depth) im Zusammenhang mit der Sicherheit von Automatisierungssystemen wie folgt:

…"Sicherheitsarchitektur, die von der Annahme ausgeht, dass jeder Punkt, der eine Schutzmaßnahme darstellt, überwunden werden kann und wahrscheinlich überwunden wird." (ANSI/ISA-99, 2007)

Das Konzept hat folgende Kennzeichen:

- Ein Angreifer muss bei der Durchbrechung oder Umgehung der einzelnen Schutzschichten damit rechnen, dass er entdeckt wird.
- Eine Schwachstelle in einer Schicht muss durch die Abwehrmöglichkeiten in einer anderen Schicht geschlossen werden.
- Die Systemsicherheit bildet innerhalb der Netzwerksicherheit eine eigene Schichtenstruktur.

Das mehrschichtige Konzept geht von der Annahme aus, dass jeder Angriff beim Versuch eine oder mehrere Schichten zu durchbrechen, entdeckt wird und der Angriff durch weitere Sicherheitsmaßnahmen abgewehrt werden kann.

Die tiefgestaffelte Verteidigung mit mehreren Verteidigungslinien wird als generelles Sicherheitskonzept in der IT-Sicherheit angewandt, denn Sicherheit wird niemals durch eine Einzelmaßnahme erreicht.

[23] Das American National Standards Institute (ANSI) ist ein Normungsinstitut der USA

Das Idaho National Laboratory hat dieses universelle schichtbasierte Verteidigungsprinzip für SCADA-Systeme grundsätzlich definiert.

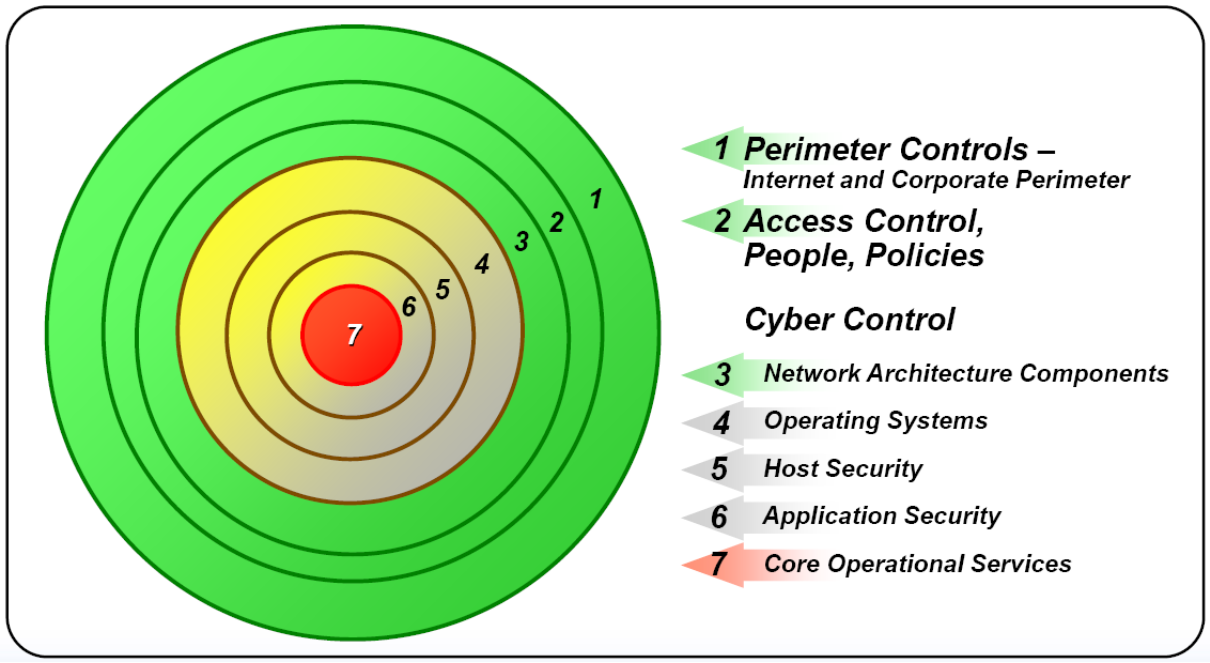

Abbildung 19: Defense in Depth nach INL (INL, 2007)

Der Kern des Systems wird mit seinen Funktionen und Diensten durch gestaffelte Verteidigungslinien geschützt. Auf eine genaue Definition der Verteidigungsmaßnahmen wird hierbei nicht eingegangen.

Siemens hat die Strategien von Defense in Depth im Sicherheitskonzept für die SCADA-Systeme PCS 7 und WinCC (Siemens, 2008) für jede Zugriffsart auf das System genau definiert.

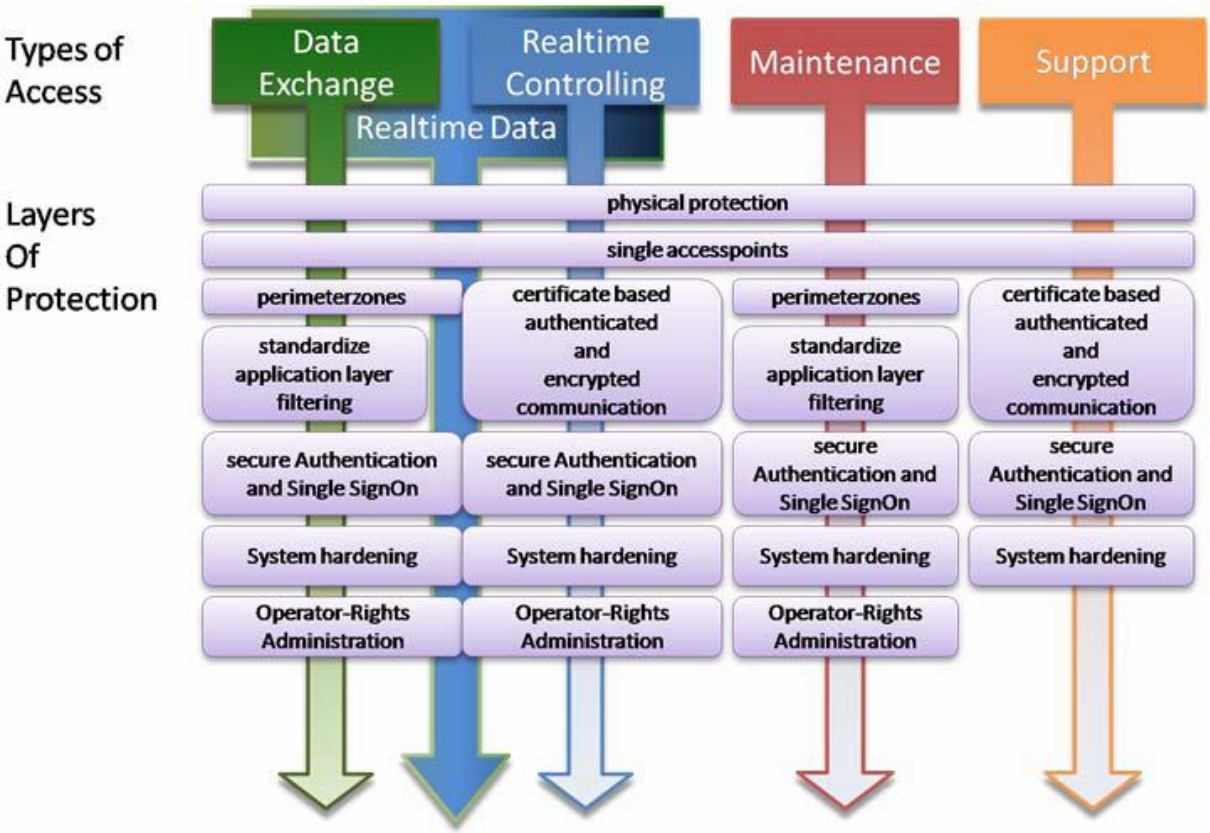

Abbildung 20: Defense in Depth für WinCC (Siemens, 2008)

Das Sicherheitskonzept unterscheidet dabei folgende Zugriffsarten:

- **Data Exchange (Daten- und Informationsaustausch)**
  Austausch von Informationen zwischen verschiedenen Produktionsebenen (z.B. Automatisierungs- und Leitebene), Anlagen und Security-Zellen
- **Realtime Controlling (Steuern)**
  Steuern oder Remoteunterstützung
- **Maintenance (Wartung)**
  Datensicherung, Updates und Konfigurationen
- **Support (technische Unterstützung)**
  Engineering, Upgrades, Änderungen am System, Fehlerdiagnose und –korrektur

Zugriffe dürfen nur über eindeutig authentisierte Netzwerkgeräte oder Benutzer erfolgen. Die Verteidigungsschichten gliedern sich in:

- **Physischer Zugangsschutz**
  Gebäude, Räume, Schränke, Geräte und Kabel müssen durch geeignete Maßnahmen geschützt werden. Der Zugangsschutz von dezentralen Anlagen und Betriebsmitteln darf auf keinen Fall vernachlässigt werden.
- **Ein Zugriffspunkt (Single Access Point)**
  Für jede Security-Zelle (siehe Absatz 6.2) sollte nur ein Zugriffspunkt (über Firewall) existieren, an dem sich Geräte, Benutzer und Anwendungen authentisieren, um Zugriff zu erlangen.
- **DMZ (Perimeterzonen-Technik)**
  Der externe Zugriff auf Daten sollte immer über eine DMZ erfolgen (siehe Absatz 2.1.1.4).
- **Application Layer Firewall**
  Application Layer Firewalls (siehe Absatz 2.1.1.3) sollten wenn möglich eingesetzt werden.
- **Zertifikatsbasierte authentisierte und verschlüsselte Kommunikation**
  Die Verwendung von sicheren Protokollen wie IPsec und SSL sollte erzwungen werden, wenn DMZ- und AFL-Techniken nicht verfügbar sind.
- **Sichere Authentisierung und Einmalanmeldung (Single Sign-on)**
  Durch den Einsatz von Single Sign-on Technologie wird die Benutzerverwaltung (z.B. Passwortrichtlinie) vereinfacht. Der Einsatz muss durch den Systemhersteller unterstützt werden.
- **Systemhärtung (Hardening)**
  Systemhärtung ist das Einschränken und Deaktivieren von nicht unbedingt benötigten Programmen und Diensten sowie das Patchen von Betriebssystem und Anwendungen.
- **Verwaltung der Bedienerberechtigungen (Rollenbasierte Zugriffssteuerung)**
  Benutzer dürfen nur die für ihre Rolle benötigten Rechte haben.

6.2 Security-Zellen

Durch die Schaffung von aufgabenorientierten Security-Zellen wird die Gesamtverfügbarkeit des Systems erhöht und der Wirkungsbereich bei Sicherheitsereignissen begrenzt. Security-Zellen sind autarke Automatisierungszellen, die durch Sicherheitsmaßnahmen wie z.B. durch Firewalls getrennt sind.

Automatisierungszellen müssen folgende Bedingungen erfüllen:

- Automatisierungszellen müssen eine Zeit lang autark betriebsfähig sein, wenn z.B. die WAN-Verbindung oder eine Firewall ausfällt. Sie sollten also einer funktionsfähigen Anlage oder Teilanlage entsprechen.
- Die Komponenten einer Automatisierungszelle müssen direkt miteinander verbunden sein, z.B. über ein LAN. Der Einsatz von gemieteten Verbindungen innerhalb einer Zelle ist unzulässig, da diese als nicht vertraulich eingestuft werden müssen.
- Anlagenteile, die eine hohe Netz- oder Rechenbelastung erzeugen, sollten innerhalb einer Zelle sein, um die Firewall nicht zu überlasten.

Automatisierungszellen dürfen zu einer Security-Zelle zusammengefasst werden, wenn folgende Bedingungen erfüllt sind:

- Der Zugang zu einer Security-Zelle darf nur durch vertrauenswürdige Personen mit entsprechender Einweisung erfolgen.
- Der Zugriff von Personen und Geräten ist nur nach erfolgreicher Authentisierung möglich.
- Jeder Zugriff muss protokolierbar oder überwachbar sein.

Security-Zellen (Siemens, 2008)

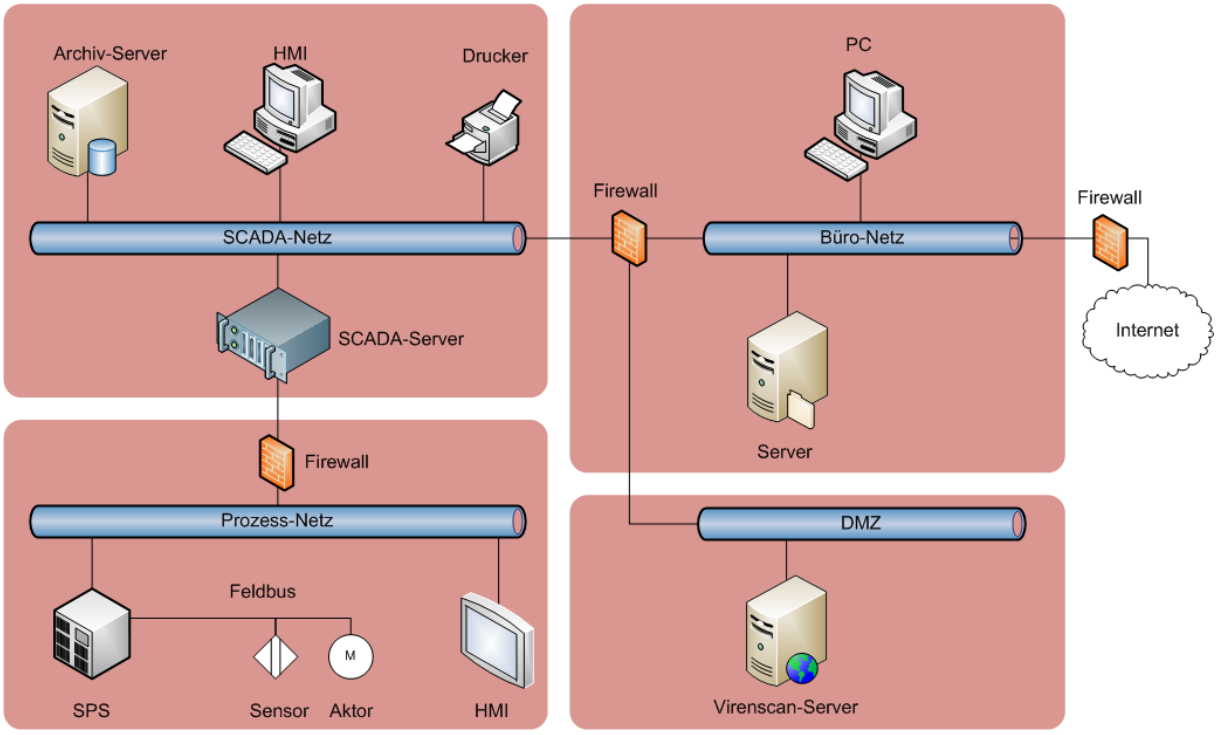

Abbildung 21: Trennung des Netzes in Security-Zellen

Beispiele für Automatisierungszellen in einer Anlage sind:

- Maschinensteuerungen
- Wehrsteuerungen
- Wasserwirtschaftsautomatik
- Schaltanlagen

Beispiele für Security-Zellen im Anlagenverbund sind:

- SCADA-System einer Zentralwarte
- Kraftwerk
- Umspannwerk
- DMZ
- Office-LAN

6.3 Sichere Zugriffstechniken

Abhängig von der Zugriffsart nach dem Konzept der tiefgestaffelten Verteidigung (siehe Abbildung 20) werden unterschiedliche Zugriffstechniken angewandt. (Siemens, 2008)

6.3.1 Wartungszugang

Externe Wartungszugänge sollten folgende Kriterien erfüllen:

- Der Zugriff sollte nur über verschlüsselte VPN-Verbindungen und Firewall erfolgen.
- zwingende Authentisierung des Benutzers an der Firewall
- Nutzung von perimetergesicherten Terminalservern oder Engineering-Systemen, um auf SCADA-System zuzugreifen

Für den Zugriff sollte ein nur für diesen Zweck definierter Wartungsrechner verwendet werden, da seine Konfiguration und Sicherheitsniveau bekannt sind und so das Risiko geringer ist. Die direkte Einwahl eines Wartungsrechners auf Systeme im Produktions-Netz ist nicht sicher, da der Zugriff nur sehr schwer eingeschränkt werden kann.

6.3.2 Abgesetzte HMIs und Engineering-Systeme

Abgesetzte HMIs und Engineering-Systeme stellen hohe Ansprüche an das Sicherheitskonzept einer Anlage, da eine missbräuchliche Verwendung großen Schaden verursachen kann. Meist werden die Gefahren, die durch den Betrieb von dezentralen, abgesetzten Arbeitsplätzen entstehen, unterschätzt. Bei mangelhaftem physischem Zugriffsschutz könnte von einem ungeschützten abgesetzten Arbeitsplatz in das System unzulässig eingegriffen werden. Arbeitsplätze sind daher mit Autologout-Funktion oder zumindest mit automatischem Bildschirmschoner mit Passwortschutz auszustatten.

Die Kommunikation über Security-Zellen hinweg ist mit Zertifikaten zu authentisieren und zu verschlüsseln.

6.3.3 Webveröffentlichung

Laut Siemens (Siemens, 2008) ist die Webveröffentlichung eine der modernsten und sichersten Zugriffstechniken. Die Produktionsdaten werden hierbei auf einem in der DMZ situiertem Web-Server geschrieben. Der Lesezugriff vom Office-Netzwerk auf den Web-Server sollte über die Firewall und SSL gesichert erfolgen.

6.4 Virenschutz

Die oberste Priorität von SCADA-Systemen ist die Überwachung und Steuerung von Prozessen. Diese Aufgabe darf durch den Einsatz von Virenschutzmechanismen nicht nachteilig beeinträchtigt werden. Ein inadäquates Virenschutzkonzept könnte den sicheren Betrieb der Anlage gefährden.

Selbst Hersteller von SCADA-Systemen können die Auswirkungen von Virenschutzprogrammen auf das Echtzeitverhalten und die Performance häufig nur schwer abschätzen. Die Implementierung eines nicht freigegebenen Virenschutzprogramms kann zum Garantieverlust der Anlage führen und sollte daher vorher mit dem Hersteller oder Lieferanten abgeklärt werden. Meist sind vor der Einführung von Virenschutzmaßnahmen umfangreiche Tests notwendig, da SCADA-Systeme häufig kunden- und aufgabenspezifisch konfiguriert sind. Generell sind Windows-basierte Betriebssysteme durch den Verbreitungsgrad entsprechender Viren und Schadprogramme stärker betroffen als Unix-basierte Systeme.

Virenschutzprogramme für Produktionssysteme sollten laut (Siemens, 2008) folgende Anforderungen erfüllen:

- Das Erkennen eines Virus darf nur eine Hintergrundalarmierung auslösen. Das Verdecken von Prozessinformationen durch Pop-ups ist unzulässig.
- Alle Meldungen sollten am zentralen Virenscan-Server protokolliert werden.
- Das übliche Blockieren, Verschieben oder Löschen von infizierten Dateien muss deaktivierbar sein.
- Alle Funktionen, die über einen klassischen Virenscanner hinausgehen, müssen deaktivierbar sein (z.B. E-Mail-Scan).
- Der Virenscanner sollte aus Performancegründen nur den eingehenden Datenverkehr überprüfen. Voraussetzung dafür ist, dass die lokalen Daten bereits manuell überprüft wurden.
- Der Virenscanner sollte aus Performancegründen nur lokale Medien überprüfen.
- Die automatische Verteilung der Virensignaturen muss deaktivierbar sein. Des Weiteren muss die Verteilung manuell und gruppenbasiert durchführbar sein.

Ein herkömmlich konfigurierter Virenschutz würde den Zugriff auf eine infizierte Datei verweigern und den Benutzer zu weiteren Maßnahmen (blockieren, verschieben oder löschen) auffordern. An einem SCADA-HMI könnte das zum Absturz führen. Hier muss der Virenschutz so parametriert werden, dass eine erfolgreiche Virenerkennung nur eine Alarmierung des Systembetreuers auslöst. Der ordnungsgemäße Betrieb des HMI muss zu jeder Zeit gesichert sein.

Die bevorzugte Architektur besteht aus einem Virenscan-Server zur zentralen Verwaltung der Virenscan-Clients und Bereitstellung der aktuellen Virensignaturen. Der Virenscan-Server sollte in einer DMZ situiert sein, da er seine Virensignaturen über das Internet vom Update-Server des Herstellers bezieht. Durch das Bilden von Test- und Produktivgruppen können neue Signaturen auf Systemverträglichkeit getestet werden, bevor sie auf den Produktivsystemen eingespielt werden.

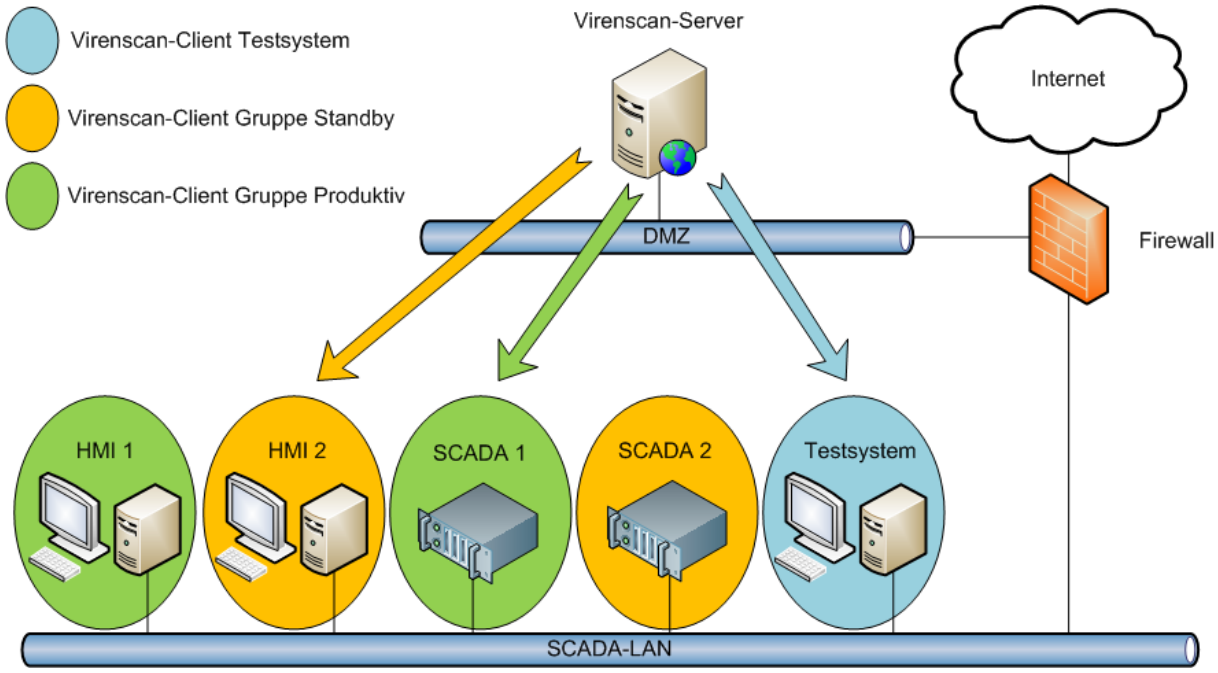

Abbildung 22: Virenschutzarchitektur

6.5 Patch-Management

Durch das Einspielen von Softwareaktualisierungen (Patches) werden bekannt gewordene Sicherheitslücken geschlossen. Patches können dabei das Betriebssystem oder die darauf laufenden Applikationen betreffen. Ein Angreifer kann in Abhängigkeit von der Art und Schwere der Sicherheitslücken in einem ungepatchten System durch einen Exploit (siehe Absatz 4.1.2) eindringen oder Schaden anrichten. Aber auch das unkontrollierte Einspielen von Patches ohne vorbereitende Maßnahmen kann schwerwiegende Auswirkungen haben. Nicht getestete Patches könnten zu Fehlfunktionen in SCADA-Systemen führen. Ein Hersteller oder Lieferant könnte etwaige Garantieansprüche durch den Betreiber bei nicht autorisiertem Patchlevel der Anlage verweigern. Durch die lange Lebensdauer von SCADA-Systemen kann es passieren, dass der Support für Applikation oder Betriebssystem eingestellt wurde und keine adäquaten Patches für bekannt gewordene Sicherheitslücken zur Verfügung stehen. In solchen Fällen sollte das dadurch entstandene Risiko kalkuliert und in Abhängigkeit von Kosten und Nutzen Maßnahmen, wie z.B. ein Systemupgrade, gesetzt werden. (NIST SP800-82, 2008)

Um den sicheren Betrieb der Anlage zu gewährleisten, sollte das Patchen nach folgender Vorgangsweise erfolgen:

- Auswahl relevanter Patches (nur wichtige sicherheitsrelevante Patches)
- Rücksprache mit dem Hersteller oder Lieferanten des Systems
- Backup der Systeme
- Testen von freigegebenen Patches auf Testsystemen
- Einspielen und Testen der Patches auf Standby-Systemen
- Einspielen der Patches auf Produktivsystemen

Ein vorhandener Notfallplan sollte die Wiederherstellung des Systems bei missglücktem Patch-Vorgang sicherstellen.

7 Zusammenfassung

Das Ziel dieser Arbeit war die Beleuchtung, der für SCADA-Systeme relevanten Aspekte der IT-Sicherheit, um in weiterer Folge eine Risikoanalyse am System der Zentralwarte Steiermark durchführen zu können. Dazu wurden einführend die Grundlagen von IT-Sicherheit und SCADA-Systemen erörtert.

IT-Sicherheit wird durch einen kontinuierlichen Prozess, bei dem die drei Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit von IT-Werten zu schützen sind, gewahrt. Dabei werden technische, organisatorische und personelle Maßnahmen eingesetzt. Um den Sicherheitsprozess geeignet steuern zu können, sollte dies im Rahmen eines IT-Sicherheitsmanagementsystems geschehen. Das Gesamtrisiko eines Informationsverbundes sollte, durch eine Risikoanalyse erfasst, bewertet und mit daraus resultierenden Maßnahmen, reduziert werden. Grundlegende technische Schutzmaßnahmen wie Zugriffskontrolle, Virenschutz, Firewall, DMZ, IDS/IPS, virtuelles LAN und VPN stellen die Basis der IT-Sicherheitsmaßnahmen dar.

Die für die IT-Sicherheit maßgeblichen Normen sind in der Reihe ISO/IEC 27000 festgehalten. Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) hat die mit der ISO/IEC-Normenreihe 27000 konformen BSI-Standards 100, für den praxisorientierten Einsatz herausgegeben. Das „National Institute of Standards and Technologie“ (NIST) der USA hat im Jahr 2008 mit der „Special Puplication 800-82, Guide to Industrial Control Systems (ICS) Security“ (NIST SP800-82, 2008) einen englischsprachigen Leitfaden veröffentlicht, der sich explizit mit der Sicherheit von SCADA-Systemen beschäftigt.

Mit SCADA-Systemen werden häufig dezentrale technische Prozesse, die der kritischen Infrastruktur eines Staates oder einer Organisation zugerechnet werden, zentral überwacht und gesteuert. Dadurch haben SCADA-Systeme aus Sicht der IT-Sicherheit einen erhöhten Schutzbedarf.

Aufgrund ihrer historischen Entwicklung und ihrer im Vergleich zu Office-IT langen Lebensdauer, haben heute in Betrieb befindliche SCADA-Systeme häufig schwerwiegende Sicherheitsdefizite. Sie wurden auf Verfügbarkeit und Leistung aber nicht auf IT-Sicherheit konzipiert. Das Sicherheitskonzept beschränkte sich auf den Schutz des physischen Zugangs. Das Bedrohungsbild hat sich durch zunehmende Verbreitung von Informationstechnologie seither aber grundlegend verändert. Die zunehmende Vernetzung von ehemals autarken SCADA-Systemen und der Office-IT setzt diese den Gefahren der modernen IT-Welt aus.

Der Einsatz von heute als unsicher geltenden Diensten, Protokollen und Methoden verschärft diese Situation weiter.

Die zahlreichen Unterschiede zwischen Systemen der Office-IT und Produktions-IT (siehe Absatz 2.2.3) erfordern den behutsamen Einsatz von IT-Sicherheitskonzepten und Techniken im Umfeld von SCADA-Systemen.

Die Erhebung des aktuellen Stands der Technik von SCADA-Systemen zeigt auf, dass Punkt-zu-Punkt-Verbindungen zunehmend durch Ethernet-Protokolle abgelöst werden. Als Plattform kommen immer häufiger Windows-basierte Betriebssysteme mit all ihren Vorteilen (bekanntes Look and Feel, einfacher Datenaustausch) und Nachteilen (Viren- und Patchproblematik) zum Einsatz. Durch die Integration von teilweise unsicheren Webtechnologien, wie z.B. ActiveX oder Java, werden erweiterte Anforderungen abgedeckt.

Bei der Analyse der Bedrohung von SCADA-Systemen wurde die Gruppe der vorsätzlichen Handlungen genauer betrachtet. Dies würde im englischen Sprachraum dem Bereich der IT-Security entsprechen. Das Spektrum der möglichen Angreifer reicht von Malware Autoren bis zu ausländischen Geheimdiensten. Die dabei eingesetzten Methoden, wie z.B. Malware oder DoS-Attacken, zielen darauf ab Informationen zu erlangen, zu zerstören, zu verändern, Dienste zu blockieren oder Funktionen lahm zu legen.

Die Eintrittswahrscheinlichkeit von Angriffen wurde vom Idaho National Laboratory (INL) untersucht. Angreifer und deren Methoden wurden in 3 Gruppen eingeteilt. Dabei ist die Wahrscheinlichkeit, von generellen, nicht strukturierten Angriffen bedroht zu werden, am höchsten. Die Konsequenzen sind hierbei aber als geringfügig einzustufen. Bei zunehmender Komplexität der Angriffe und steigenden Konsequenzen für das attackierte System, sinkt jedoch die Wahrscheinlichkeit von einem solchen Angriff bedroht zu werden, da solche Angriffe mehr Wissen und Mittel benötigen.

Der Bedrohungsursprung veränderte sich laut einer Studie des British Columbia Institute of Technologie (BCIT) (BCIT, 2004) stark hin zu externen Angriffen. Viele Angriffe laufen heutzutage automatisiert ab und sind nicht zielgerichtet. SCADA-Systeme werden dabei eher zufällig als absichtlich zum Ziel. Durch die fortschreitende Vernetzung der Systeme wurden Angriffsflächen geschaffen, der sich die Betreiber oft nicht bewusst sind. Die genauere Untersuchung der internen Sicherheitsereignisse zeigt, dass diese überwiegend aus dem Office-Netz kommen, der interne Einsatz von Firewalls ist daher unumgänglich. Bei den externen Sicherheitsereignissen stellt das Internet gefolgt von Einwahl-Modems die größten Gefahrenquellen dar. Grundsätzlich gibt es eine große Anzahl von Möglichkeiten, um in das Produktionsnetz einzudringen. Es reicht daher nicht aus, die Sicherheitsanstrengungen auf

einen Zugangspunkt zu konzentrieren, weil dabei viele andere Zugangsmöglichkeiten außer Acht gelassen werden und das Restrisiko für die Anlage beträchtlich bleibt.

Die Bedrohungsentwicklung laut BSI (BSI, 2009b) muss als kritisch betrachtet werden, da die Prognose viele Gefährdungen als steigend einstuft. Dies trifft im Besonderen auf SCADA-Systeme zu.

Mögliche Angriffsszenarien wurden vom „United States General Accounting Office“ (GOA) im Jahr 2004 (GOA, 2004) untersucht. Die Palette der Szenarien reicht vom Blockieren des Datenflusses über das Ändern von Programmcodes bis hin zum Einschleusen von falschen Prozessinformationen, um gefährliche Bedienhandlungen zu provozieren.

Die Analyse von bekannten sicherheitsrelevanten Ereignissen führt die Bildung des Sicherheitsbewusstseins beim Leser fort. Die in der „Industrial Security Incident Database“ (ISID) erfassten Ereignisse wurden vom BCIT auf Häufigkeit untersucht (BCIT, 2004). Dabei wurde um das Jahr 2003 ein signifikanter Anstieg der Ereignisse festgestellt. Die Autoren führen dies auf den unbedarften Einsatz neuer Technologien, wie z.B. Internet und zunehmende Vernetzung, zurück. Erst durch die Implementierung von geeigneten Sicherheitsmaßnahmen wurde diesem Trend entgegengewirkt. Eine Reihe von bekannt gewordenen Ereignissen zeigt in weiterer Folge, dass Schwachstellen und sorgloses Agieren in der Vergangenheit bereits zu teilweise ernsthaften Vorfällen geführt haben.

In weiterer Folge wurden in der Arbeit typische SCADA-Schwachstellen erhoben. Das NIST (NIST SP800-82, 2008) teilt diese in die 3 Kategorien Richtlinien und Prozeduren, Plattform und Netzwerk ein.

Die häufigsten Schwachstellen von SCADA-Systemen sind:

- fehlende SCADA-spezifische Richtlinien, Prozeduren und Trainings
- schlechte Netzwerkarchitektur ohne tiefgestaffelte Verteidigung
- zunehmende Vernetzung und Vermischung des Datenverkehrs zwischen Prozess- und Office-Netzen
- Einsatz von ungeschützten Remote-Zugängen und unsicheren Übertragungsprotokollen
- unzureichender physischer Zugangsschutz zu Systemen, Netz- und Übertragungseinrichtungen
- Verwendung von unsicheren Protokollen und Technologien, dessen Spezifikationen leicht zugänglichen sind
- Fehlen von Malwareschutz, IDS-Systemen und Ereignisprotokollierung

- Informationen über Architektur, Betriebsweise, Vernetzung und Kommunikationstechnik sind über Internet leicht verfügbar
- mangelndes Sicherheitsbewusstsein bei Betreibern und Lieferanten

Im abschließenden Kapitel dieser Diplomarbeit wurden auf SCADA-Systeme abgestimmte Sicherheitskonzepte und Schutzmaßnahmen betrachtet.

Das universelle, mehrschichtige Konzept der tiefgestaffelten Verteidigung (Defense in Depth) geht von der Annahme aus, dass jeder Angriff beim Versuch eine oder mehrere Schichten zu durchbrechen, entdeckt wird und der Angriff durch weitere Sicherheitsmaßnahmen abgewehrt werden kann. Es setzt sich aus mehreren hintereinander gestaffelten Schichten zusammen, die einzelne oder mehrere Schutzmaßnahmen repräsentieren. Sicherheit wird niemals durch eine Einzelmaßnahme erreicht.

Durch die Bildung von Security-Zellen kann der Wirkungsbereich bei Sicherheitsereignissen begrenzt werden. Diese Netzwerkarchitekturmaßnahme lässt autarke Automatisierungszellen nur über definierte Schnittstellen (Firewalls) kontrolliert kommunizieren.

Der Einsatz von sicheren Zugriffstechniken soll die Integrität und Verdaulichkeit des Systems auch bei externen Wartungszugriffen, abgesetzten Arbeitsplätzen und Datenaustausch gewähren. Als Sicherheitsmaßnahmen kommen hierbei Verschlüsselung, VPN-Verbindungen, Perimetertechnik, Firewalls und Zertifikate zum Einsatz.

Virenschutzmaßnahmen müssen in der Umgebung von Produktionssystemen behutsam eingesetzt werden. Die Verfügbarkeit der Systeme hat oberste Priorität. Die eingesetzten Virenscanner müssen den Anforderungen der SCADA-Hersteller bzw. Lieferanten entsprechen. Die auf SCADA-Systeme abgestimmte Konfiguration darf den sicheren Betrieb auch bei erfolgreicher Virenerkennung nicht negativ beeinflussen. Auf die speziellen Echtzeitanforderungen der SCADA-Systeme muss Rücksicht genommen werden. Mit einer strukturierten Updatestrategie der Virenschutzclients kann die Systemverträglichkeit sichergestellt werden.

Ein geeignetes Patch-Management stellt das Schließen von sich auftuenden Sicherheitslücken in Betriebssystem und Applikationen sicher. Häufig laufen SCADA-Systeme ohne jemals gepatcht worden zu sein.

Generell müssen IT-Sicherheitsmaßnahmen der Office-IT an die speziellen Anforderungen von SCADA-Systemen angepasst werden. Dabei ist die interdisziplinäre Zusammenarbeit von Experten der IT, SCADA-Spezialisten und Operatoren notwendig.

Sicherheit lässt sich nicht nur allein durch technische Maßnahmen erreichen, es müssen auch organisatorische und personelle Aspekte betrachtet werden. Nur durch Einführung und

Betrieb eines IT-Sicherheitsmanagementsystems kann die Sicherheit auf Dauer auf einem angemessenen Niveau garantiert werden.

Im Zuge der Literaturrecherche wurde festgestellt, dass sich relevante Quellen hauptsächlich im amerikanischen Raum mit der Sicherheit von SCADA-Systemen intensiver auseinandersetzen. Dies hat wahrscheinlich mit den Terroranschlägen vom 11. September 2001 oder dem Northeast Power Blackout von 2003 und dem dadurch angestiegenen Sicherheitsbewusstsein amerikanischer Behörden und Betreiber zu tun. Im deutschsprachigen Raum wird diesem Thema noch wenig Beachtung geschenkt.

8 Bewertung der erreichten Ziele und Ausblick

In dieser Arbeit wurden die Grundlagen und der Stand der Technik von IT-Sicherheit und SCADA-Systemen strukturiert dargestellt und in Zusammenhang gebracht. Im Weiteren wurde auf die Unterschiede zwischen Office- und Produktions-IT aufmerksam gemacht. Das Hauptziel - die Darstellung von Bedrohungspotenzial, typischen Schwachstellen und Schutzmaßnahmen - wurde durch die Recherche von anerkannten Quellen wie z.B. die des BSI, der ISO und des NIST erreicht. Dabei ist anzumerken, dass das konkrete Bedrohungspotenzial für SCADA-Systeme nur schwer einschätzbar ist, da Eintrittswahrscheinlichkeiten nur geschätzt werden können und tatsächlich eingetretene sicherheitsrelevante Vorfälle nur selten an die Öffentlichkeit gelangen. Die in Absatz 3.2 definierten Ziele wurden in den Kapiteln 4, 5 und 6 erläutert. In Kapitel 7 wurden die wichtigsten Erkenntnisse in kompakter Form wiedergegeben.

Zusammenfassend kann gesagt werden, dass durch die Eingrenzung der Thematik auf die Kerninhalte der für ein SCADA-System relevanten Risikofaktoren und der damit zusammenhängenden Problemerfassung mit der vorliegenden Arbeit ein Ansatz für die Problembehebung erarbeitet wurde. Es wurde anhand der durchgeführten Literaturrecherche, der kritischen Auseinandersetzung mit anerkannten Quellen und der systematischen Darstellung der vorliegenden Problematik ein leicht verständliches Werk zum Thema SCADA-Sicherheit geschaffen. Diese Arbeit kann somit als fundierte Basis für die geplante Risikoanalyse am SCADA-System der Zentralwarte Steiermark herangezogen werden. Die angeführten Literaturquellen können als Ausgangspukt für weitere Untersuchungen im Zusammenhang mit dem Thema SCADA-Sicherheit dienen.

Ausblick

Nach der am SCADA-System durchzuführenden Risikoanalyse sollte die Erstellung eines Sicherheitskonzeptes für die Wartenleitsysteme im Unternehmen folgen. Die anschließende Umsetzung des daraus resultierenden IT-Sicherheitsplanes sollte im Rahmen eines einzuführenden IT-Sicherheitsmanagementsystems erfolgen.

Weiterführende IT-Sicherheitsuntersuchungen könnten im Themenbereich der Fernwartung stattfinden, da sich hier im Unternehmen gerade ein Technologiewechsel vollzieht. Es sollen schmalbandige RAS-Zugänge auf der Basis von ISDN durch breitbandig an das Internet angebundene virtualisierte Fernwartungsanwendungen ersetzt werden. Dadurch kann der sichere externe Wartungszugriff auf Prozess- und Wartenleitsysteme des Unternehmens für Lieferanten und Mitarbeiter über Internetanbindung gewährleistet werden.

Literaturverzeichnis

ABB. 2009. *Industrial IT System 800xA.* [Online] 2009. [Zitat vom: 15. Sept. 2009.] http://www.abb.de/product/ge/9AAC115756.aspx.

ANSI/ISA-99. 2007. Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models. 2007.

BCIT. 2004. The Myths and Facts behind Cyber Security Risks for Industrial Control Systems. *British Institute of Technologie.* [Online] April 2004. [Zitat vom: 15. Okt. 2009.]

BSI. 2008. BSI-Leitfaden zur Einführung von Intrusion-Detection-Systemen. [Online] 2008. [Zitat vom: 13. Sept. 2009.] https://www.bsi.bund.de/cln_134/ContentBSI/Publikationen/studien/ids02/gr1_htm.html.

BSI. 2009a. Definition Kritische Infrastrukturen. [Online] 2009a. [Zitat vom: 3. Sept. 2009.] https://www.bsi.bund.de/cln_136/ContentBSI/Themen/kritis/Einfuehrung/KritisDefinitionen/definitionen.html.

BSI. 2009b. Lagebericht. [Online] 2009b. [Zitat vom: 15. Okt. 2009.] https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html.

BSI. 2009c. Organisationsübersicht des BSI. [Online] 2009c. [Zitat vom: 12. Okt. 2009.] https://www.bsi.bund.de/cln_136/DE/dasBSI/Aufgaben/aufgaben_node.html.

BSI-100-1. 2008. Managementsysteme für Informationssicherheit (ISMS). *BSI-Standard 100-1.* [Online] Version 1.5, Mai 2008. www.bsi.bund.de.

BSI-100-2. 2008. IT-Grundschutz-Vorgehensweise. *BSI-Standard 100-2.* [Online] Version 2.0, Mai 2008. www.bsi.bund.de.

BSI-GSK. 2009. IT-Grundschutz-Kataloge. [Online] BSI, Sept. 2009. https://www.bsi.bund.de/cln_136/DE/Themen/weitereThemen/ITGrundschutzKataloge/itgrundschutzkataloge_node.html.

CNN. 1998. *Teen hacker faces federal charges.* [Online] Cable News Network (CNN), 18. März 1998. [Zitat vom: 28. Okt. 2009.] http://www.cnn.com/TECH/computing/9803/18/juvenile.hacker/index.html.

Der Standard. 2009. Georgien-Konflikt tobt auch im Internet. [Online] 2009. [Zitat vom: 20. Okt. 2009.] http://derstandard.at/fs/1216918992632.

Federrath, Hannes und Pfitzmann, Andreas. 2004. Datenschutz und Datensicherheit. [Hrsg.] Uwe Schneider und Dieter Werner. *Taschenbuch der Informatik.* 5. Auflage. München : Carl Hanser Verlag, 2004, 15, S. 467-488.

GE. 2009. *XA/21 SCADA / Energy Management System.* [Online] 2009. [Zitat vom: 24. Nov. 2009.] http://www.gepower.com/prod_serv/products/scada_software/en/xa21.htm.

GE Fanuc. 2009. *Proficy HMI/SCADA - iFIX.* [Online] 2009. [Zitat vom: 15. Sept. 2009.] http://www.gefanuc.com/products/3311.

GOA. 2004. Challenges and Efforts to Secure Control Systems. *United States General Accounting Office.* [Online] 2004. [Zitat vom: 26. Okt. 2009.] http://www.gao.gov/new.items/d04354.pdf.

Heise. 2009. *Drei Viertel der Admins trauen dem Virenscanner nicht.* [Online] 2009. [Zitat vom: 25. Sept. 2009.] http://www.heise.de/newsticker/meldung/Drei-Viertel-der-Admins-trauen-dem-Virenscanner-nicht-755737.html.

Henning, Peter A. 2004. Internet und Intranet. [Hrsg.] Uwe Schneider und Dieter Werner. *Taschenbuch der Informatik.* 5. Auflage. München : Carl Hanser Verlag, 2004, S. 359-388.

HMS. 2009. Industrial Ethernet im Überblick . [Online] HMS Industrial Networks GmbH, 2009. [Zitat vom: 14. Sept. 2009.] http://www.anybus.de/technologie/ethernet.shtml.

INL. 2009. About INL. [Online] Idaho National Laboratory, 2009. [Zitat vom: 27. Okt. 2009.] https://inlportal.inl.gov/portal/server.pt?open=512&objID=259&parentname=CommunityPage&parentid=1&mode=2&in_hi_userid=2&cached=true.

INL. 2007. Control Systems Cyber Security for Managers and Operators. *Idaho National Laboratory.* [Online] 2007. [Zitat vom: 27. Okt. 2009.] http://www.inl.gov/scada/training/d/4hr_introductory_scada_security.pdf.

ISO. 2009. About ISO . [Online] Sept. 2009. [Zitat vom: 6. Okt. 2009.] http://www.iso.org/iso/about.htm.

Kaspersky, Eugene. 2008. *Malware: Von Viren, Würmern, Hackern und Trojanern und wie man sich vor ihnen schützt.* München : Hanser Fachbuch, 2008.

Meyers, Mike und Harris, Shon. 2007. *CISSP Certified Information Systems Secuity Professional.* [Übers.] Rolf von Rössing und Markus a Campo. 2. Auflage. Heidelberg : mitp, 2007.

Microsoft TechNet. 2006. Einführung in VLANs. [Online] 2006. [Zitat vom: 28. Sept. 2009.] http://www.microsoft.com/germany/technet/itsolutions/network/grundlagen/tec_comp_3_2_1.mspx.

Müller, Heinz. 2004. Multimedia. [Hrsg.] Uwe Schneider und Dieter Werner. *Taschenbuch der Informatik.* 5. Auflage. München : Carl Hanser Verlag, 2004, S. 556 - 587.

NIST SP800-53. 2009. *Recommended Security Controls for Federal Information Systems and Organizations (SP800-53).* Gaithersburg, USA : National Institute of Standards and Technology, 2009.

NIST SP800-82. 2008. *Guide to Industrial Control Systems (ICS) Security (SP 800-82).* Gaithersburg, USA : National Institute of Standards and Technology, 2008.

Oechsle, Rainer. 2004. Verteilte Systeme. [Hrsg.] Uwe Schneider und Dieter Werner. *Taschenbuch der Informatik.* 5. Auflage. München : Carl Hanser Verlag, 2004, S. 389-417.

OE-IT-SIHB. 2007. Österreichisches Informationssicherheitshandbuch. [Online] Version 2.3, April 2007. http://www.digitales.oesterreich.gv.at/site/5261/default.aspx.

OPC Foundation. 2009. What is OPC? [Online] 2009. [Zitat vom: 6. Okt. 2009.] http://www.opcfoundation.org/Default.aspx/01_about/01_whatis.asp?MID=AboutOPC.

Sandia National Laboratories. 2005. Penetration Testing of Industrial Control Systems. [Online] März 2005. [Zitat vom: 29. Okt. 2009.] http://www.sandia.gov/scada/documents/sand_2005_2846p.pdf.

SecurityFocus. 2003. *Slammer worm crashed Ohio nuke plant network.* [Online] 19. Aug. 2003. [Zitat vom: 28. Okt. 2009.] http://www.securityfocus.com/news/6767.

Siemens. 2008. Sicherheitskonzept PCS 7 und WinCC. [Online] 2008. [Zitat vom: 5. Nov. 2009.] http://support.automation.siemens.com/WW/view/de/26462131.

Siemens. 2009a. SIMATIC HMI. [Online] 2009a. [Zitat vom: 15. Sept. 2009.] http://www.automation.siemens.com/hmi/index_00.htm.

Siemens. 2009b. SINAUT Spectrum / Spectrum Power 4. [Online] 2009b. [Zitat vom: 15. Sept. 2009.] https://w3.energy.siemens.com/cms/00000020/de/produkte/netzleittechnik/sinautspectrum/Seiten/sinautspectrum.aspx.

Siemens. 2009c. Spectrum PowerCC Energy Control / SCADA. [Online] 2009c. [Zitat vom: 15. Sept. 2009.] https://www.energy.siemens.com/cms/00000029/Pages/products.aspx?lang=de&partid=SPCEC&uid=13491409141013405&country=ZZ.

Tauchnitz, Thomas und Maier, Uwe. 2008. Prozessleitsysteme. [Hrsg.] Karl Friedrich Früh, Uwe Maier und Dieter Schaudel. *Handbuch der Prozessautomatisierung: Prozessleittechnik für verfahrenstechnische Anlagen.* 4. Auflage. s.l. : Oldenbourg Industrieverlag, 2008.

TecChannel. 2003. *MS-SQL Slammer: Ein Wurm und die Konsequenzen.* [Online] TecChannel, 28. Jan. 2003. [Zitat vom: 28. Okt. 2009.] http://www.tecchannel.de/sicherheit/spam/402050/ms_sql_slammer_ein_wurm_und_die_konsequenzen/index.html.

The Register. 2001. *Hacker jailed for revenge sewage attacks.* [Online] The Register, 31. Okt. 2001. [Zitat vom: 28. Okt. 2009.] http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/.

The Washington Post. 2008. Cyber Incident Blamed for Nuclear Power Plant Shutdown. [Online] 5. Juni 2008. [Zitat vom: 30. Okt. 2009.] http://www.washingtonpost.com/wp-dyn/content/article/2008/06/05/AR2008060501958.html.

U.S.-Canada Power System Outage Task Force. 2004. [Online] 2004. [Zitat vom: 28. Okt. 2009.] http://www.oe.energy.gov/DocumentsandMedia/BlackoutFinal-Web.pdf.

Verbund. 2009. Geschäftsbereiche. [Online] Sept. 2009. [Zitat vom: 07. Sept. 2009.] http://www.verbund.at/cps/rde/xchg/internet/hs.xsl/150_166.htm.

Victor, Frank. 2004. Programmiersprachen. [Hrsg.] Uwe Schneider und Dieter Werner. *Taschenbuch der Informatik.* 5. Auflage. München : Carl Hansa Verlag, 2004, S. 270 - 292.

Wiles, Jack, et al. 2007. *Techno Security's Guide to Securing SCADA.* Burlington : Syngress, 2007.

Erklärung

Ich erkläre, dass ich die vorliegende Arbeit selbständig und nur unter Verwendung der angegebenen Literatur und Hilfsmittel angefertigt habe.

Graz, 15. Jänner 2010